Defense Information Systems Agency

A Combat Support Agency

NETWORK SERVICES DIRECTORATE (NS)

ENTERPRISE CONNECTION DIVISION (NSC)

CONNECTION PROCESS GUIDE

Version 3.2

May 2011

Defense Information Systems Agency
Enterprise Connection Division (NSC)
Post Office Box 4502
Arlington, Virginia 22204-4502
www.disa.mil/connect

EXECUTIVE SUMMARY

This Connection Process Guide (CPG) implements the requirement in Department of Defense Directive (DoDD) 8500.01E *Information Assurance (IA)*, 24 October 2002 (ref c), DoD Instruction (DoDI) 8500.02 *Information Assurance (IA) Implementation*, 6 February 2003 (ref f), and CJCSI 6211.02C *Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 (ref a), that Director, Defense Information Systems Agency (DISA), establish, manage, maintain, and promulgate a customer connection process guide describing steps that must be followed to request and implement a DISN connection. The goal of the CPG is to describe a transparent, user-friendly, and agile process that will help the warfighter and mission partners, as defined in directive DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009 (ref n), get connected quickly, and in a manner that does not bring an unacceptable level of risk to the DISN at large. This release of the CPG:

- Updates and cancels the previous DISN Connection Process Guide, May 2010.
- Outlines the step-by-step process that all DoD and non-DoD mission partners, which includes non-DoD federal agencies, state and local government activities, contractors, foreign entities, etc., must follow. While the connection process can be complex, close adherence to the procedures described in this guide will ensure the most expeditious and secure completion of required tasks.
- Adds or revises several specific areas to include:
    - Improving clarity of the non-DoD connection request letter to Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII)
    - Specifics on the network/topology diagram requirements for package submission

This guide is approved for public release and is available on the Internet from the DISA website at http://www.disa.mil/connect.

The instructions in this guide are effective immediately.

SIGNATURE PAGE FOR KEY OFFICIALS

Approved by:

____ ________________________

Chief, Enterprise Connection Division **Date**

REVISION HISTORY

This document will be reviewed and updated as needed (minimum quarterly). Critical and Substantive changes will be reflected in the revision history table.

Version	Date	Comments
3.0	May 2010	Baseline document released based on stakeholder input and extensive reformatting.
3.1	April 2011	Administrative changes to incorporate current policy and correct errors.
3.2	May 2011	Updated telephone numbers due to DISA BRAC relocation to Ft. Meade, MD.
	May 2011	Change DISN Customer Contact Center (DCCC) to DISN Global Support Center (DGSC).

This page intentionally left blank.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

This page intentionally left blank.

SECTION 1
INTRODUCTION

1.1 Purpose

The security of cyberspace is a Presidential national security priority and all DoD components must work together to provide the vital security elements to DoD's portion of cyberspace – the Defense Information Enterprise, which includes the DISN. Fundamentally, cyberspace is made possible by the billions of various connections that make up the fabric of this truly global infrastructure. Stated simply, our combined connection approval actions significantly influence the security of the Defense Information Enterprise as a part of cyberspace. Together we must take this responsibility seriously and perform the necessary due diligence to ensure all the appropriate policies, procedures, and guidelines are followed. In short, there is a reason behind DoD's IA strategy, architecture, governance, and policies, such that every time the warfighter presses the "push to talk" button or the "Enter" key, they are ultimately connected clearly, reliably, and securely to the sovereign power of the United States.

The CPG is a step-by-step guide to the detailed procedures that all DoD and non-DoD mission partners must follow to obtain and retain connections to the DISN. The guide consolidates the connection processes for all networks and services into one document, helps customers understand connection requirements and timelines, and provides contacts for assistance throughout the process. The Enterprise Connection Division is not the process owner for the entire "connection process"; the CPG points customers to appropriate information services, websites, or offices wherever possible to help guide customers through the entire process.

Deriving authority from DoDD 8500.01 *Information Assurance (IA),* 24 October 2002 (ref c), DoDI 8500.02 *Information Assurance (IA) Implementation*, 6 February 2003 (ref f), and CJCSI 6211.02C *Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 (ref a), this guide is a living document that continues to evolve as connection processes for existing networks/services are refined and as additional networks/services become available. While this version of the CPG is limited to the DISN as detailed below, future versions of the CPG will expand to cover DoD's ever-evolving capabilities such as Unified Capabilities (UC), layer 3 VPNs, and cloud computing.

Use and consult the CPG often to assist you through the connection process. However, before employing this guide, always check for the current version on our website at: http://www.disa.mil/connect.

DISN networks/services and controlled processes addressed in this guide are included in Table 1.

DISN Network/Service	Classification Supported
Cross Domain Solutions (CDS)	SECRET/Unclassified
Defense Red Switched Network (DRSN)	SECRET
Defense Switched Network (DSN)	Unclassified
DISN Leading Edge Services (DISN-LES)	SECRET
DISN Video Services (DVS)	SECRET/Unclassified
Non-Classified Internet Protocol Router Network (NIPRNet)	Unclassified
Office of the Secretary of Defense (OSD) Global Information Grid (GIG) Waiver Process	Unclassified
Real Time Services (RTS)	SECRET/Unclassified
Secret Internet Protocol Router Network (SIPRNet)	SECRET
Secure Mobile Environment-Portable Electronic Device (SME-PED)	SECRET/Unclassified

Table 1 DISN Networks/Services and Supported Classification

1.2 Applicability

This guide applies to all DoD and non-DoD information systems (ISs) seeking to connect to the DISN. For definitions and descriptions of a DoD IS and a non-DoD entity, refer to DoDD 8500.01E *Information Assurance (IA)*, 24 October 2002 (certified current as of 23 April 2007) (ref c), and CJCSI 6211.02C *Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 (ref a), respectively.

1.3 Document Structure

The document is organized as follows:

SECTION 1 defines the purpose, applicability, and structure of this guide.

SECTION 2 provides a high-level overview of the process all customers must follow to obtain and retain a connection to the DISN.

SECTION 3 contains DISN Connection Process details in flowchart and text format. It addresses the common process mechanisms and requirements for DoD and non-DoD customers, regardless of which network/service is needed. This section does not include information on the unique steps for obtaining a connection to a specific network/service (e.g., SIPRNet, DISN Video Services – Global (DVS-G), etc.).

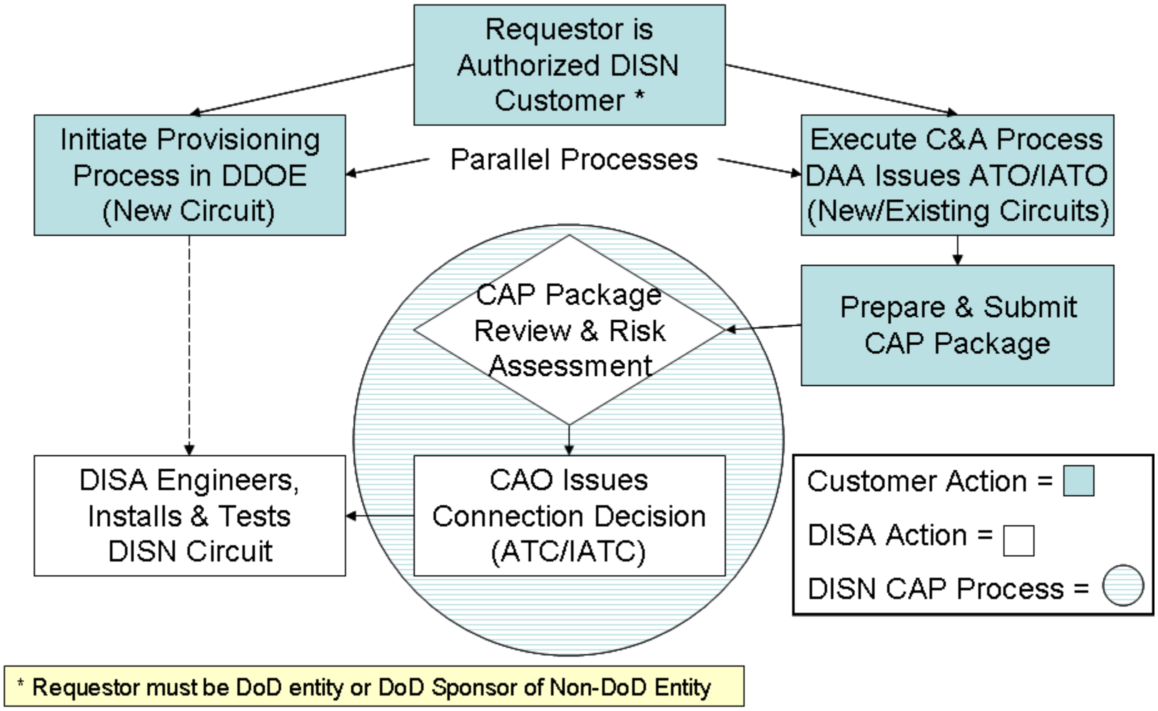
The Appendices contain the Non-DoD Connection Validation Template, the Non-DoD Connection Revalidation Template, individual appendices defining DISN network/service-specific connection requirements, policy references (including hyperlinks to access the most current policy documents), acronym definitions, and a glossary of terms. Network/service-specific appendices also include web links to additional resources and DISN network/service point of contact (POC) information.

SECTION 2

DISN CONNECTION PROCESS OVERVIEW

This section presents a high-level overview of the DISN connection process, focusing on the key areas that the customer must thoroughly understand and properly execute to obtain and retain a connection to the network/service appropriate for their mission.

Figure 1 provides a graphical depiction of the overall process.


Requestor is Authorized DISN Customer *
Initiate Provisioning Process in DDOE (New Circuit)
Parallel Processes
Execute C&A Process DAA Issues ATO/IATO (New/Existing Circuits)
CAP Package Review & Risk Assessment
Prepare & Submit CAP Package
DISA Engineers, Installs & Tests DISN Circuit
CAO Issues Connection Decision (ATC/IATC)
Customer Action = 🟦
DISA Action = □
DISN CAP Process = ○

* Requestor must be DoD entity or DoD Sponsor of Non-DoD Entity

Figure 1 High-Level DISN Connection Approval Process (CAP)

2.1 Key Connection Process Areas and Terms

2.1.1 DISN Technical Fundamentals

The DISN has the following generalized components:

- Long-haul transport (Wide Area Network (WAN))
- Components to manage/operate the long-haul transport
- Services that are enabled on the long-haul transport (Network Enabled Services)
- Enclaves that derive access to the network-enabled services by connecting Local Area Networks (LANs) to the WAN to gain access to WAN services; enclaves may include voice, video, email, Web access, and other services in the local environment; enterprise-level services, such as Cross Domain Enterprise Services, Defense Enterprise Computing Centers (DECC), Network Operations Centers (NOC), Teleport, etc.

2.1.2 DISN Customers

There are two types of customers that connect to the DISN to utilize its networks/services: DoD and non-DoD. DoD customers are DoD Combatant Commands, Military Services and Organizations, Agencies, and Field Activities (DoD CC/S/A/FA), which are collectively referred to as "DoD Components." Per Reference (a) in the **Error! Reference source not found.** appendix, non-DoD customers include all organizations and entities that are not components of the DoD. This includes contractors and federally funded research and development centers; other U.S. government federal departments and agencies; state, local, and tribal governments; foreign government organizations/entities (e.g., allies or coalition partners); non-government organizations; commercial companies and industry; academia (e.g., universities, colleges, or research and development centers); etc. Non-DoD customers must have a validated requirement approved by a sponsoring CC/S/A or field activity headquarters and approval from the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD(NII)/DoD Chief Information Officer (CIO)).

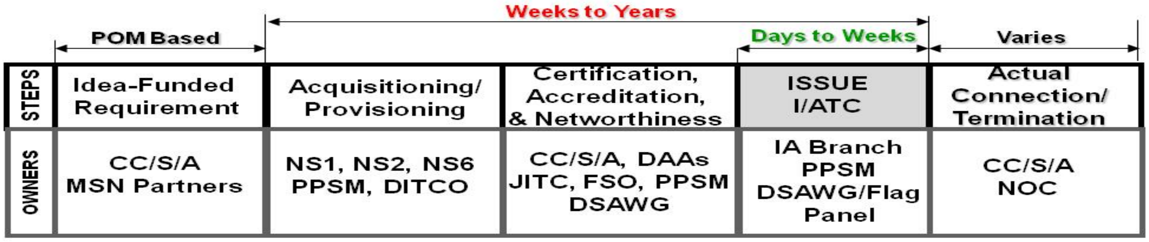
2.1.3 DISN Networks/Services and Connections

The DISN offers classified and unclassified voice, video, and data services to its customers. A detailed description of each of the services is available at the following website: http://www.disa.mil/services/index.html?panel=10#A_Services. Each service requires specific types of network connections to access and utilize the service. Connection types are described in the appendix corresponding to each specific service.

2.1.4 Request Fulfillment (Formerly called Provisioning)

Customers requiring a new connection to the DISN and its services must use the DISA Direct Order Entry (DDOE) request fulfillment process to initiate circuit activation (see the DDOE website, https://www.disadirect.disa.mil/products/asp/welcome.asp, for further information and guidance). Request fulfillment involves the ordering, engineering, acquisition, and installation of the circuit and equipment necessary to connect to the DISN. Request fulfillment may only be initiated by a DoD entity. A DoD entity may sponsor a non-DoD entity, but the DoD entity remains responsible for all request fulfillment actions, and, in some cases, all Certification and Accreditation (C&A) actions. See Section 3.2.8 for more information on C&A requirements.

A very simplified conceptual customer view of the request fulfillment process shows the end-to-end length of time a complete connection can take, and all the various steps and process owners that can influence the process. This diagram is by no means all-inclusive, nor does it attempt to represent the request fulfillment process for all connections in DoD. The request fulfillment process does not end with the actual connection because the C&A cycle repeats until the IS is physically disconnected. See Figure 2.



STEPS	Idea-Funded Requirement	Acquisitioning/ Provisioning	Certification, Accreditation, & Networthiness	ISSUE I/ATC	Actual Connection/ Termination
OWNERS	CC/S/A MSN Partners	NS1, NS2, NS6 PPSM, DITCO	CC/S/A, DAAs JITC, FSO, PPSM DSAWG	IA Branch PPSM DSAWG/Flag Panel	CC/S/A NOC

Figure 2 Request Fulfillment (or Connection) Process

2.1.5 DISN Network/Service Specific Requirements

While all DISN networks/services follow similar connection process steps, there may be network/service-specific requirements for requesting and obtaining a connection, e.g., registering the connection request in an IS/database dedicated to that network/service and/or ensuring components are listed on the DoD Approved Products List (APL) prior to purchase or lease, as designated in each network/service-specific appendix. The common connection process steps are presented in Section 3, while any unique network/service-specific requirements are provided in the appendices.

2.1.6 Certification and Accreditation (C&A)

All ISs, including network enclaves connecting to the DISN, require certification and accreditation in accordance with an appropriate and acceptable process. **For new and additional circuits, the IS C&A process should be initiated parallel to or soon after beginning the request fulfillment process.** For existing circuits, the customer should initiate IS reaccreditation actions with sufficient time prior to expiration of the current accreditation and connection approval to prevent a circuit disconnect action.

DoD entities must execute the DoD Information Assurance Certification and Accreditation Process (DIACAP). For non-DoD entities, the appropriate C&A process depends on the type of non-DoD entity and the network/service to be accessed, as described in Section 3. At the completion of the C&A process, the Designated Accrediting Authority (DAA) issues an accreditation decision in the form of an Authorization to Operate (ATO), Interim ATO (IATO), or Interim Authorization to Test (IATT). This artifact (for DIACAP actions -- the signed Scorecard) is required in the Connection Approval Process (CAP) package before an Approval to Connect (ATC) or Interim ATC (IATC) can be issued by the DISN Connection Approval Office (CAO).

2.1.7 Connection Approval Office (CAO)

The Enterprise Connection Division's Information Assurance (IA) Branch has two distinctly different functions/teams: Connection Approval and Cross Domain Solutions (CDS). The CAO is responsible for processing GIG waivers, reviewing, and approving all routine DISN connection requests, which are primarily addressed in this CPG. The CAO also receives some other types of connection requests that are not routine, in the sense that they involve a higher level of risk to the DISN than the CAO is authorized to accept. Those requests (e.g., CDS) are reviewed/approved by the Defense IA/Security Accreditation Working Group (DSAWG), and in cases of even higher risk, by the DISN/GIG Flag Panel.

2.1.8 Connection Approval Process (CAP) Package

Connection requests are sent to the CAO in the form of a CAP package. These packages provide the CAO the information necessary to make the connection approval decision. The baseline requirements for what must be included in the CAP package depend on whether the customer is DoD or non-DoD and whether the connection is new or existing. There may also be additional requirements, depending on the specific DISN network/service the customer needs to access. The baseline requirements are provided in Section 3 of this guide. Any additional network/service-specific requirements are provided in the appendix that corresponds to that specific network/service.

2.1.9 Risk Assessment

As an integral part of the connection approval process, the CAO conducts an initial assessment of the risk that a new or existing connection presents to the DISN community at large. Risk assessments are based on the level of customer compliance with governance, DISA/FSO Security Technical Information Guides (STIGs), USCYBERCOM Fragmentary Orders (FRAGOs) and Communications Tasking Orders (CTOs), on-site and remote compliance monitoring and vulnerability assessment scans, DSAWG/Flag Panel decisions, etc.

When non-compliance issues are identified and confirmed, the CAO works with the customer and others to validate and correct the weaknesses that generated the risk. Weaknesses can include, among other elements, incomplete and/or incorrect information submitted as part of the CAP package documentation and artifacts.

2.1.10 Connection Decision

After the CAP package is reviewed and the risk assessment conducted, the CAO makes a connection decision and notifies the customer. Customers approved for connection to the DISN are granted either an ATC or an IATC, which is normally assigned an expiration date to coincide with the Authorization Termination Date (ATD) of the customer IS ATO or IATO. In the event of a high risk assessment for a new connection, the CAO works with the customer to address the issue until the risk can be downgraded or mitigated, allowing the issuance of an ATC or IATC.

A high risk assessment made at the time the customer requests a new approval to connect for an existing connection (or at any time during the life cycle of the connection) will also prompt the CAO to work closely with the customer to downgrade or mitigate the risk. If this is not possible due to the nature of the risk or to the customer’s inability or failure to perform due diligence in seeking resolution of the issue, the continued presence of a high risk may result in the issuance of a Denial of Approval to Connect (DATC).

The CAO will normally issue a DATC only after the DSAWG has evaluated the CAO risk assessment and judged the risk to the DISN to be unacceptable. The DSAWG will then direct the CAO to forward the DATC to the IS/enclave DAA, with an information copy to the applicable DoD Component CIO and USCYBERCOM (USCC). The DATC will normally include a request (and in cases of extreme non-compliance, a directive) that the IS/enclave be disconnected from the applicable DISN network/service.

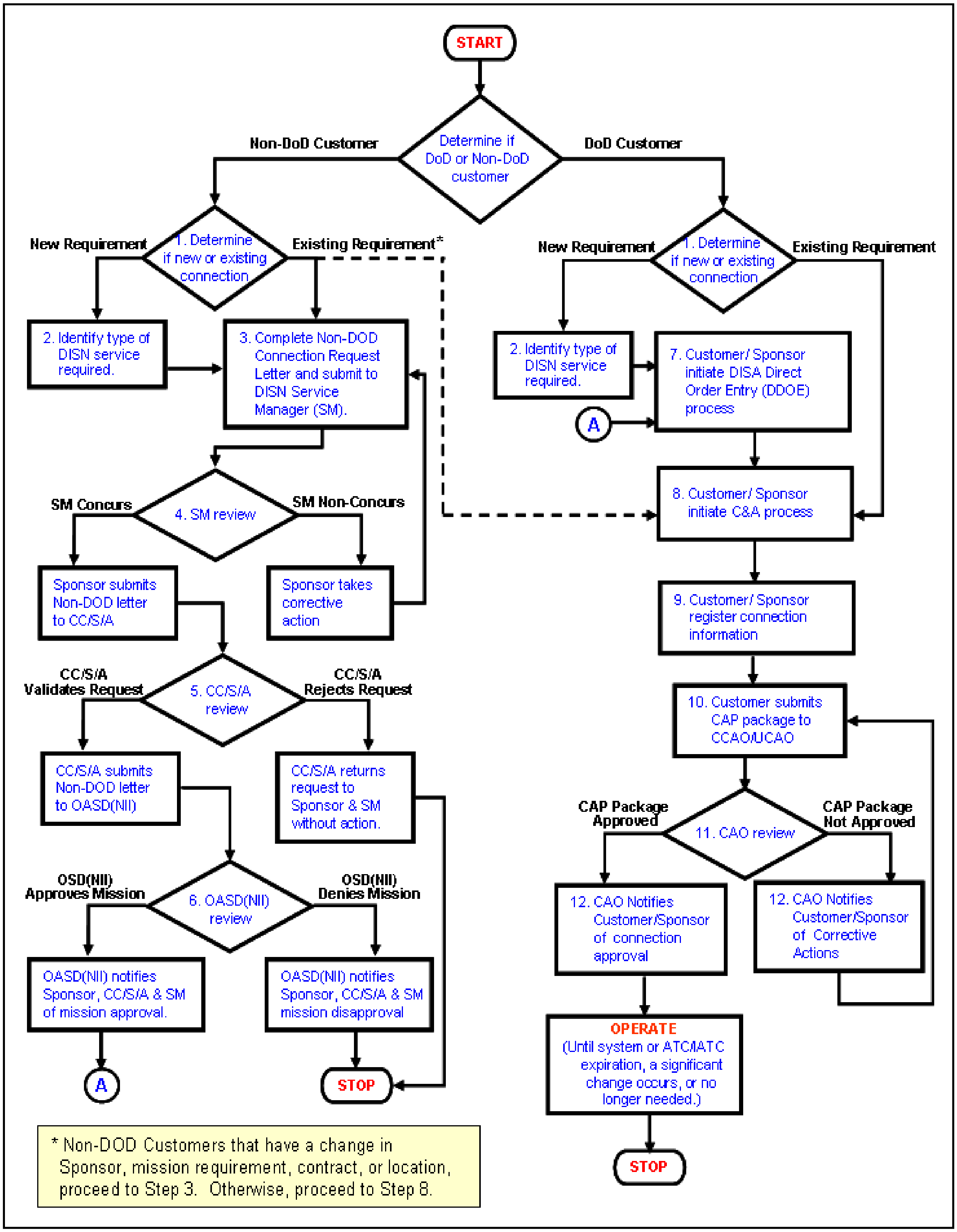
SECTION 3

DISN CONNECTION PROCESS DETAILS

The process for network/service request fulfillment and approval of a connection to the DISN or service varies depending on: 1) whether the customer is a DoD entity or a non-DoD entity; 2) whether the request is for a new connection or for an expiring existing connection; and 3) what network/service is being accessed. This section describes the connection process requirements and steps that are common to all networks/services, and addresses both new and existing connections.

3.1 DISN Connection Process Flow

The overall flow for the DISN connection process is illustrated in Figure 3. Each step within the process flow diagram includes a step number that correlates to the detailed descriptions in Section 3.2.


START
Determine if DoD or Non-DoD customer
Non-DoD Customer
DoD Customer
New Requirement
1. Determine if new or existing connection
Existing Requirement*
2. Identify type of DISN service required.
3. Complete Non-DOD Connection Request Letter and submit to DISN Service Manager (SM).
SM Concurs
4. SM review
SM Non-Concurs
Sponsor submits Non-DOD letter to CC/S/A
Sponsor takes corrective action
CC/S/A Validates Request
5. CC/S/A review
CC/S/A Rejects Request
CC/S/A submits Non-DOD letter to OASD(NII)
CC/S/A returns request to Sponsor & SM without action.
OSD(NII) Approves Mission
6. OASD(NII) review
OSD(NII) Denies Mission
OASD(NII) notifies Sponsor, CC/S/A & SM of mission approval.
OASD(NII) notifies Sponsor, CC/S/A & SM mission disapproval
A
STOP
New Requirement
1. Determine if new or existing connection
Existing Requirement
2. Identify type of DISN service required.
7. Customer/ Sponsor initiate DISA Direct Order Entry (DDOE) process
A
8. Customer/ Sponsor initiate C&A process
9. Customer/ Sponsor register connection information
10. Customer submits CAP package to CCAO/UCAO
CAP Package Approved
11. CAO review
CAP Package Not Approved
12. CAO Notifies Customer/Sponsor of connection approval
12. CAO Notifies Customer/Sponsor of Corrective Actions
OPERATE (Until system or ATC/IATC expiration, a significant change occurs, or no longer needed.)
STOP

* Non-DOD Customers that have a change in Sponsor, mission requirement, contract, or location, proceed to Step 3. Otherwise, proceed to Step 8.

Figure 3 Customer Connection Process

3.2 DISN Connection Process Steps

3.2.1 Step 1 Determine if New Connection or Existing Connection Requirement

Regardless of whether or not the customer is DoD or non-DoD, to initiate the connection process, the customer/sponsor must first determine if this is a requirement for a new connection or the modification or renewal of an existing connection.

New Connections
For customers with a new connection requirement, it is necessary to start the process from the beginning.

Both DoD and non-DoD new connection customers proceed to Step 2.

Existing Connection
If an accreditation decision is approaching its ATD, the DAA must reinitiate the C&A process and issue a new accreditation decision. Ideally, the new ATO/IATO will be issued and an updated CAP package forwarded to the CAO at least 30 days prior to the expiration of the current ATC/IATC.

The expiration date of an ATC/IATC will normally be the same as (and will never go beyond) the expiration date of the associated ATO/IATO. In some instances, the results of the CAO or DSAWG risk assessment may warrant the issuance of an ATC/IATC with a validity period shorter than that of the associated ATO/IATO. An expired ATC/IATC will prompt a review by USCYBERCOM, and will likely result in an order to disconnect the IS/enclave from the DISN network/service. See Step 11 for details.

A DAA may also decide that planned changes to an IS/enclave are significant enough to warrant reinitiating the full C&A process, with subsequent issuance of a new accreditation decision inside the normal 3-year ATO (or 180-day IATO) cycle. If no physical reconfiguration of the DISN circuit is needed to effect the planned changes, such modifications to an IS/enclave (even if significant enough to warrant a new accreditation decision) do not need to be coordinated with the corresponding DISN Service Manager (SM). The planned events may, however, have a significant impact on the IA status of the IS/enclave, and consequently on the risk the IS/enclave poses to the DISN community at large. Cases such as this prompt a requirement for the customer/sponsor to coordinate with the CAO prior to customer implementation of the change.

Examples of high-impact events requiring pre-coordination with the CAO are:

- Deployment of a cross domain solution (CDS)
- Deployment of a major Automated Information System (AIS) application, even if the application is already accredited by the IS/enclave DAA

  NOTE: The deployment to a customer enclave of an AIS accredited by the DISA DAA for DISN/GIG Enterprise deployment generally does not trigger a requirement for pre-coordination with the CAO prior to deployment.

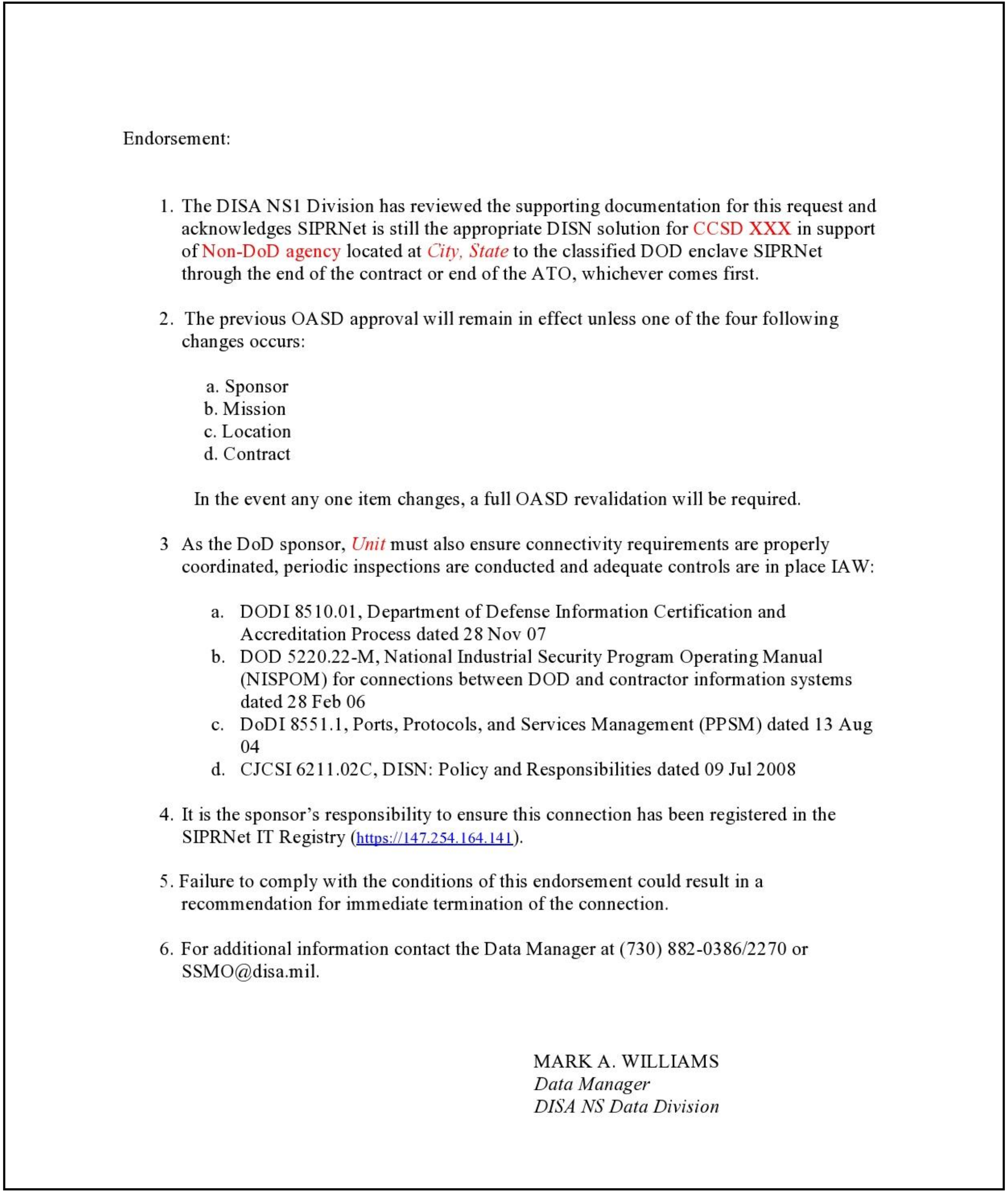
Such changes require pre-coordination because they will (in the case of a CDS) or may (in the case of a major AIS application deployment) increase the level of risk that the IS/enclave will pose on the DISN community at large. Other high-impact events (e.g., changes to the existing accreditation boundary) will also require pre-coordination with the CAO (and in the case of non-DoD connections, approval by OASD(NII) as described below) prior to implementation as they may also increase the level of community risk.

Examples of medium-impact events that pose a lesser risk to the DISN are:

- Deployment of additional workstations with new hardware and new approved/accredited software
- Changes in the IP address range assigned to the IS/enclave
- DISA transport re-homing actions that change entry points and DISN, not the customer enclave

These events do not need to be pre-coordinated with the CAO prior to deployment/implementation. deployment/implementation. However, these events must be identified to the CAO no later than deployment/implementation by providing an updated network topology diagram, as in the workstation

workstation example in



Endorsement:

1. The DISA NS1 Division has reviewed the supporting documentation for this request and acknowledges SIPRNet is still the appropriate DISN solution for CCSD XXX in support of Non-DoD agency located at *City, State* to the classified DOD enclave SIPRNet through the end of the contract or end of the ATO, whichever comes first.

2. The previous OASD approval will remain in effect unless one of the four following changes occurs:

   a. Sponsor
   b. Mission
   c. Location
   d. Contract

   In the event any one item changes, a full OASD revalidation will be required.

3 As the DoD sponsor, *Unit* must also ensure connectivity requirements are properly coordinated, periodic inspections are conducted and adequate controls are in place IAW:

   a. DODI 8510.01, Department of Defense Information Certification and Accreditation Process dated 28 Nov 07
   b. DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DOD and contractor information systems dated 28 Feb 06
   c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
   d. CJCSI 6211.02C, DISN: Policy and Responsibilities dated 09 Jul 2008

4. It is the sponsor's responsibility to ensure this connection has been registered in the SIPRNet IT Registry (https://147.254.164.141).

5. Failure to comply with the conditions of this endorsement could result in a recommendation for immediate termination of the connection.

6. For additional information contact the Data Manager at (730) 882-0386/2270 or SSMO@disa.mil.

MARK A. WILLIAMS
Data Manager
DISA NS Data Division

Figure 10.

Low-impact events, such as the one-for-one replacement of workstations with updates of similar hardware and updates of the same approved/accredited software, have no appreciable effect on the risk to the DISN. Low-impact events do not need to be communicated to the CAO until the updated information is included in the next iteration of C&A documents/artifacts provided in the connection renewal CAP package.

The examples of high-impact, medium-impact, and low-impact events described above are not all-inclusive. The DAA should evaluate whether planned changes will, in any way, affect the risk to the IS/enclave and/or the DISN/GIG at large. If the answer is "yes," customers should contact the CAO for assistance in determining what category of impact (high, medium, or low) the event falls under and the required level of coordination with the CAO.

Documentation and IA requirements for renewal approvals for existing DoD and non-DoD connections to DISN networks/services are generally the same as for new connections, including the requirement for a risk assessment by the CAO. See Step 11 for the risk assessment indicators. An ATC/IATC will not be issued in the event of a "high" risk assessment. The "high" risk condition must be reduced to allow downgrading to a "medium" or "low" risk.

There are instances where existing non-DoD connections to the DISN require re-initiation of the new connection request process. These include:

- Change in the customer's mission requirement
- For contractor connections, expiration/cancellation of the contract and/or a new contract award or significant modification, or change in contractor network location or enclave boundary

Under these circumstances, non-DoD customers/sponsors proceed to Step 3. Otherwise, both DoD and non-DoD customers/sponsors proceed to Step 8.

3.2.2 Step 2 Identify the Type of DISN Network/Service Required

Once the customer/sponsor determines that this is a new connection requirement, the next step is to identify the DISN network/service that is required. This involves matching customer needs to the most appropriate DISN network/service. All customers/sponsors desiring connections to the DISN must first confirm with the applicable SM that the desired network/service is appropriate for the mission.

Customers/sponsors who are not sure which network/service best meets their needs should review the description of DISN voice, video, and data services available at http://www.disa.mil/services/index.html?panel=10#A_Services and/or contact the DISN Global Support Center (DGSC). The DGSC will facilitate contact with the appropriate DISN SM.

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Classified email	DGSC@cols.disa.smil.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

Customers/sponsors who know which DISN service they require will find POCs for each of the DISN networks/services in this guide's individual appendices.

DoD customers proceed to Step 7.

Non-DoD customers proceed to Step 3.

3.2.3 Step 3 Complete and Submit the Non-DoD Connection Validation Letter

The sponsor may download the Non-DoD Connection Validation Letter from the DISA Connection Library at www.disa.mil/connect/library. An example is located in Appendix A. The sponsor sends the completed letter, with an attached conceptual network topology diagram, to the appropriate SM. The purpose of the conceptual network topology diagram is to provide the SM enough information to determine if their network/service is appropriate for the customer's mission. A detailed topology diagram is required in the CAP package, as discussed in Step 10.

3.2.4 Step 4 DISN Service Manager Reviews Proposed Solution

The DISN SM reviews the Non-DoD Connection Validation Letter and network topology to determine whether the proposed DISN solution is appropriate.

Concurs with Solution

If the SM concurs with the request, the SM will sign the letter and return it to the validating CC/S/A.

Non-Concurs with Solution

If the SM non-concurs with the proposed solution, the request will be returned to the sponsor with comment, or routed to another SM (after notifying the sponsor) if a different network/service solution is more appropriate for the mission.

If corrective actions are required of the sponsor, return to Step 3.

3.2.5 Step 5 CC/S/A/FA Reviews Proposed Request

The CC/S/A/FA will review the sponsor's request letter and either validate or reject the request.

Validates Request

If the CC/S/A/FA validates the request, the representative will sign the letter and submit it to the OASD(NII) for DISN access approval (with a copy to the sponsor).

Rejects Request

If the CC/S/A/FA POC rejects the request, it will be returned to the sponsor without action (with a copy to the appropriate SM) and the connection request process ends at this point.

3.2.6 Step 6 OASD(NII) Reviews Proposed Mission and DISN Solution

OASD(NII) will evaluate the connection request and either approve or deny access to the DISN in support of the sponsor's mission.

Approves Request

If OASD(NII) approves the request to access the DISN, the representative will sign and forward the request letter to the DoD sponsor (with a copy to the CC/S/A/FA POC and DISN SM).

Denies Request

If OASD(NII) does not approve the request, the representative will return the request letter to the DoD sponsor without action (with a copy to the CC/S/A/FA POC and DISN SM), and the connection, as proposed, will not be allowed.

3.2.7 Step 7 Customer/Sponsor Initiates DISA Direct Order Entry (DDOE) Process

After the appropriate network/service is identified and applicable approvals are received, the customer/sponsor initiates a request for service fulfillment through the DDOE process. This is the ordering tool for DISN telecommunications services. The DDOE website is: https://www.disadirect.disa.mil/products/asp/welcome.asp.

In the event the service request qualifies as an Emergency or Essential National Security/Emergency Preparedness (NS/EP) telecommunications service, there is an expedited process available, both for service fulfillment and for connection approval.

3.2.8 Step 8 Customer/Sponsor Initiates the Certification and Accreditation Process

In parallel, or shortly after initiating the request for service through DDOE, the customer/sponsor should begin the C&A process for the IS/enclave for which a connection to the DISN is required.

NSC encourages widespread use of the Enterprise Mission Assurance Support System (eMASS), which supports the DIACAP and the formulation of the DIACAP Scorecard. DISA is required to use eMASS by internal DISA policy.

DoD Customers

DoD customers are required to use the DIACAP and to submit (at a minimum) a complete and accurate DIACAP Executive Package, which includes the following documents/artifacts.

- System Identification Profile (SIP)
- DIACAP Scorecard
- IT Security Plan of Action and Milestones (POA&M), if required

(For instructions on how to complete these requirements, see Ref (g)/DIACAP and the DIACAP Knowledge Service at https://diacap.iaportal.navy.mil/login.htm.)

Non-DoD Customers

Non-DoD customer connections to the DISN require the completion of a C&A process. In all cases, C&A document and artifact submissions must provide IA status information equivalent to the DIACAP Executive Package.

- DIACAP Executive Package (DIACAP Scorecard)
- System Identification Profile (SIP)
- IT Security POA&M, if required
- DoD contractor connection to DISN:
  - For Unclassified connections, use DIACAP (the sponsoring DoD component has responsibility for all DAA actions)
  - For Classified connections, use DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 28 February 2006 (ref p); the Defense Security Service (DSS) has responsibility for all DAA actions; see the DSS-DISA MOA for further specifics regarding non-DoD classified connections
- For non-DoD and non-IC federal departments and agencies:
  - For an IS not categorized as a National Security System (NSS), use National Institute of Standards and Technology (NIST) SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 (ref q)
  - For an IS categorized as an NSS, and IAW CNSS Policy No. 6 *National Policy on Certification and Accreditation of National Security Systems*, October 2005 (ref l), use a C&A process as determined by the Department/Agency; refer to CNSSI 4009 *National Information Assurance Glossary*, June 2006 (ref k), for the definition of an NSS
- For other non-DoD entities, the C&A process requirements and inputs will be reviewed on a case-by-case basis. Coalition and allied mission partners will follow an established national C&A process.

At the completion of the C&A process, the DAA makes an accreditation decision. An ATO decision has a maximum validity period of 3 years, while the IATO has a maximum validity period of 180 days. In accordance with the DIACAP, consecutive IATOs shall not exceed 360 days (unless approved in writing by the DoD component CIO). For DISN connection purposes, these requirements/restrictions apply to DIACAP-based submissions, as well as to submissions based on other authorized C&A processes.

3.2.9 Step 9 Customer/Sponsor Registers the Connection Information

NOTE: *This step is not required for existing connections that are already registered, unless there is a change in vital solution information, such as POC(s), accreditation information, etc. If registration information is current, proceed to Step 10.*

Customers/sponsors are required to register the connection information (new or legacy) within the following applicable systems/databases (see appendix of desired network/service for details.)

Once the DDOE process started in Step 7 has been completed with the receipt of a Command Communications Service Designator (CCSD), customers/sponsors are required to register their IS information (IP address ranges, hosts, POCs, etc.) in one of the following databases, as appropriate:

- Network Information Center (www.nic.mil) for all unclassified connections
- SIPRNet Support Center (www.ssc.smil.mil) for all classified connections
- SNAP (https://snap.dod.mil) for:
  - Voice, video, data circuit registrations and connections to unclassified networks/services
  - OSD GIG Waivers for Internet Service Provider registrations (Appendix H)
- GIAP/SGS (https://giap.disa.smil.mil) for:
  - Voice, video, and data circuit registrations and connections to classified networks/services
    NOTE: Customers/sponsors cannot register their information directly into GIAP/SGS. This must be accomplished by submitting a CAP package to include the SCQ.
  - Ports, Protocols, and Services Management (PPSM) (https://pnp.cert.smil.mil) on SIPRNet for all networks/systems ports, protocols, and services for all IP solutions or applications, including Voice over Internet Protocol (VoIP) and Voice over Secure Internet Protocol (VoSIP)

DoD policy also requires that customers/sponsors register their IS information in the following systems/databases:

- DITPR (https://ditpr.dod.mil) for all unclassified networks/systems
- SIPRNet IT Registry (https://www.itdb.itiss.osd.smil.mil) for all classified networks/systems

Additionally, CC/S/A/FAs may have other databases that need to be updated with connection information. Check with your CC/S/A/FA for additional requirements.

3.2.10 Step 10 Customer/Sponsor Submits Connection Approval Package

Customer/sponsor connection requests are submitted to the CAO in the form of a CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to expiration or desired connection date for new connections, or the expiration date of the current connection approval for existing connection.

Tactical exercise/mission CAP packages must be submitted a minimum of eight (8) days prior to the start of the exercise/mission. Tactical mission/exercise requests should include the mission number found on the Gateway Access Authorization (GAA) subject line or the timeframe of the exercise. The GAA message must be released by the Contingency and Exercise (CONEX) prior to an IATC/ATC letter being issued by the CAO.

The following documents must be included in the CAP package (see the appropriate network/service appendix for any additional requirements):

- DIACAP Executive Package (or equivalent documentation and artifacts for non-DoD connections) – contains the minimum information required for the accreditation decision and consists of the three components listed below. In accordance with Ref (g), information from DIACAP packages "is made available as needed to support an accreditation decision or other decision such as a connection approval." Furthermore, the Executive Package "contains the minimum information for an accreditation decision."
- DIACAP Scorecard – must be signed by the DAA. The signed Scorecard documents the accreditation decision, as well as the results of the implementation and verification of required IA controls. It also serves as the formal statement regarding the DAA's acceptance of any residual risk, the details for which must be provided in the IT Security POA&M. All non-compliant and N/A IA controls should also be reflected in the POA&M.
- SIP – a compiled list of system characteristics or qualities required to register an IS with the governing DoD Component IA program. Item 14 of the SIP is for Additional Accreditation Requirements. While not foreseen in the DIACAP, customers are requested to list their circuit CCSD in Item 14 of the SIP. The CCSD(s) can also be displayed in the System Description section.
  ***NOTE**: This is not in the DIACAP, but this needs to be added to the process so that the circuit can be identified on the SIP.*
- IT Security POA&M, if applicable (e.g., in the case that any baseline or other required IA controls are assessed by the Certifying Authority (CA) as being Non-Compliant (NC) (to include inherited controls), or not applicable (NA) controls.
- DAA Appointment Letter – must be included if there is a new DAA or if the information is not already on file in the CAO. The letter must appoint an official specifically by name, not the office to which the managerial official is assigned. If the DAA has delegated signature authority to an authorized official, written evidence of a delegation action must be provided to the CAO prior to the acceptance of any CAP package documentation.
- Consent-to-Monitor (CTM) – this is the agreement signed by the DAA granting DISA permission to monitor the connection and assess the level of compliance with IA policy and guidelines. CTM supports electronic monitoring for communications management

and network security, which includes site visits, compliance inspections, and remote vulnerability assessments to check system compliance with configuration standards. It is recommended that DAAs provide blanket CTM for the CCSDs under their authority.

- Network Topology Diagram – this diagram depicts the network topology and security posture of the customer IS or network enclave that will be connecting to the DISN. The drawing should be provided over SIPRNet and must:

  - Be dated
  - Clearly delineate accreditation boundaries
  - Identify the CCSDs of all connections to the DISN
  - Identify equipment inventory (to include the most recent configuration including any enclave boundary firewalls, Intrusion Detection Systems (IDS), servers, hubs, bridges, premise router, routers, major applications, gateways, modems, backup devices, room and building number, switches, backside connections, Internet Protocol (IP) addresses, encryption devices, Cross Domain Solutions (CDS), and Ports, Protocols, and Services Management (PPSM) boundary crossing/interface devices

    - ***NOTE 1***: It is important to note that in accordance with DoD and DISA guidance, firewalls and IDSs are required on all customer enclaves; approval for connection to the SIPRNet will not be granted unless an approved firewall and IDS have been included in the customer's configuration and are compliant with published guidance; private IP addresses (non-routable) are not permitted on SIPRNet enclaves
    - ***NOTE 2***: Indicate and label all of the devices, features, or information; diagram minimum size: 8.5" x 11"

  - Other SIPRNet connections (access points) must be shown; the flow of information to, from, and through all connections, host IP addresses, and CCSD number, if known must be shown
  - Identify any other IA or IA-enabled products deployed in the enclave
  - Identify any connections to other systems/networks
  - Identify Internetworking Operating System (IOS) version
  - Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)

NOTE: *The IA and IA-enabled products must be on the National Information Assurance Partnership (NIAP) Validated Products List (VPL) – see the DISA Field Security Operations (FSO) Network Security Technical Implementation Guide (STIG). The VPL is available at http://www.niap-ccevs.org/cc-scheme/vpl/. The enclave boundary firewall and IDS hardware model and software version numbers must be entered on the topology diagram. Customers must ensure the hardware and software combination is a combination that was evaluated by checking the "CC Certificate" (Common Criteria) available at the NIAP site for all validated products.*

Identification of other connected IS/enclaves must include:

- The name of the organization that owns the IS/enclave
- The connection type (e.g., wireless, dedicated point-to-point, etc.)

- IP addresses for all devices within the enclave
- The organization type (e.g., DoD, federal agency, contractor, etc.)

Refer to the applicable DISN network/service appendix for sample topology diagrams.

In addition to the above package requirements, non-DoD customers/sponsors are required to submit the following information:

- OASD(NII) Validation/Revalidation Letter – this is the letter from OASD(NII) approving access to the DISN. It is provided to the customer/ sponsor after having completed the non-DoD connection request process described above.
- Proof of Contract – if the customer requesting the connection is a DoD contractor, the sponsor must submit proof of a valid contract (normally a DD Form 254).

Additional connection-specific artifacts may be required for inclusion in the CAP package and may differ based on which DISN network/service is selected. Detailed requirements are identified in the applicable network/service appendix.

CAP packages for unclassified and classified connections should be sent to the CAO. CAP packages are normally submitted as Unclassified/For Official Use Only (FOUO). However, it is recommended that the network topology diagram be provided over SIPRNet or via encrypted email. The customer/sponsor must determine, based on DoD component and local guidance, if any part of the CAP package contents must be labeled and handled as classified documents. The CAP package submission email addresses, phone numbers, and mailing addresses are:

Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Unclassified email	UCAO@disa.mil CCAO@disa.mil	UCAO@disa.mil CCAO@disa.mil
Classified email	UCAO@disa.smil.mil CCAO@disa.smil.mil	UCAO@disa.smil.mil CCAO@disa.smil.mil
Phone (Commercial)	703-882-2086, 703-882-1455	703-882-2086, 703-882-1455, 301-225-2900/2901
Phone (DSN)	312-381-2086, 312-381-1455	312-381-2086, 312-381-1455 301-761-2900/2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 4502 Arlington, VA 22204-4502	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Ft. Meade, MD 20755-0549

3.2.11 Step 11 CAO Review of the CAP Package and the Authorization to Connect Decision

Upon receipt of the CAP package, the CAO reviews the contents and makes a connection decision. In the event an incomplete package is received by the CAO, the package will be rejected and no CAO tracking number assigned. The customer will receive notification of a rejected package to include what documentation is missing from the package. Once a complete package is received, a CAO tracking number will be assigned and a receipt notification will be provided. If further analysis identifies missing or incomplete information, a CAO analyst will coordinate with the customer POC to obtain the required information. Typically, when all the connection approval requirements are met, a new or renewal request for an existing connection will be granted, and an ATC or IATC will be issued within five (5) business days.

As an integral part of the process, the CAO assesses the level of risk the customer's IS or network enclave poses to the specific DISN network/service and to the GIG community at large. The identification of IA vulnerabilities or other non-compliance issues and the responsiveness of the affected enclave in implementing appropriate remediation or mitigation measures against validated vulnerabilities will have a direct impact on the risk assessment, and subsequently on the connection approval decision.

The following are some of the indicators that would contribute to the assessment of an elevated risk:

- Missing, incomplete, or inaccurate CAP package input (because unknowns lead to a lower level of confidence in the IA status of the customer IS/enclave).
  ***NOTE**: Missing, incomplete, or inaccurate CAP package input may result in a USCYBERCOM decision and order to disconnect the customer from the DISN.*
- Unsatisfactory results during an on-site or remote compliance monitoring/vulnerability assessment event where IA controls are tested and policy compliance is reviewed.

If the risk is "low" or "medium," the CAO will normally issue an ATC or IATC. A "medium" risk assessment will normally cause the CAO to monitor more closely the IA status of the IS/enclave during the connection life cycle. "Low" risk assessments will not affect a new request or an existing connection.

An ATC/IATC will normally authorize the customer to connect or remain connected to the DISN network/service defined in the connection approval up to the accreditation decision ATD. As stated previously, the results of the risk assessment may warrant the issuance of a connection approval decision with a validity period shorter than that of the accreditation decision ATD. In such cases, the CAO will provide justification to the DAA for the shorter validity period.

If the CAO assesses a "high" risk, it will provide the DAA the justification for the assessment and inform the DAA that current guidance (i.e., policy, DSAWG decision, STIGs, etc.) from DISN/GIG DAAs precludes the issuance of an ATC without additional review of the IS/enclave IA status by the community accreditation bodies.

The CAO will work with the customer and others (including the applicable CC/S/A/FA CIO, as appropriate) and monitor the customer's progress in correcting the non-compliance issues. If customer progress toward remediation/mitigation of the risk is unsatisfactory, the CAO will forward pertinent risk information to the DSAWG for review. If the DSAWG downgrades the assessment of high risk, the connection approval process will proceed in accordance with the procedures outlined above for medium or low risks. If the DSAWG confirms the assessment of high risk, it will instruct the CAO to issue a DATC, which includes a recommendation that USCYBERCOM issue an order that the customer IS/enclave be disconnected from the applicable network/service.

On receipt of the DATC, USCYBERCOM initiates disconnect review procedures as described in CJCSI 6211.02C *Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 (ref a).

The customer's network/service connection remains in a DATC status until it is brought into compliance or disconnected.

3.2.12 Step 12 CAO Notifies the Customer/Sponsor of Connection Approval or Denial

Once the CAO makes a connection decision, the customer/sponsor is notified.

Connection Approval

If the connection request is approved, the customer is issued an ATC or IATC. The validity period is specified in the ATC/IATC letter. After the connection is approved, the customer must work with DISN Implementation to complete the installation of the circuit. The connection approval is valid until the expiration date. The DAA must notify the CAO of significant changes, such as architecture changes requiring re-accreditation, changes in risk posture, etc., that may cause a modification in the IA status of the system/enclave or if the connection is no longer needed.

Denial of Approval to Connect

If the connection request is denied, the CAO will provide the customer/sponsor a list of corrective actions required before the connection can be approved.

Return to Step 10.

This page intentionally left blank.

APPENDIX A

NON-DOD DISN CONNECTION VALIDATION TEMPLATE

This appendix provides a sample of the template for the Non-DoD DISN Connection Validation Letter. This is the only acceptable template for this letter. Once completed, submit the letter according to the instructions identified in Section 3.2.

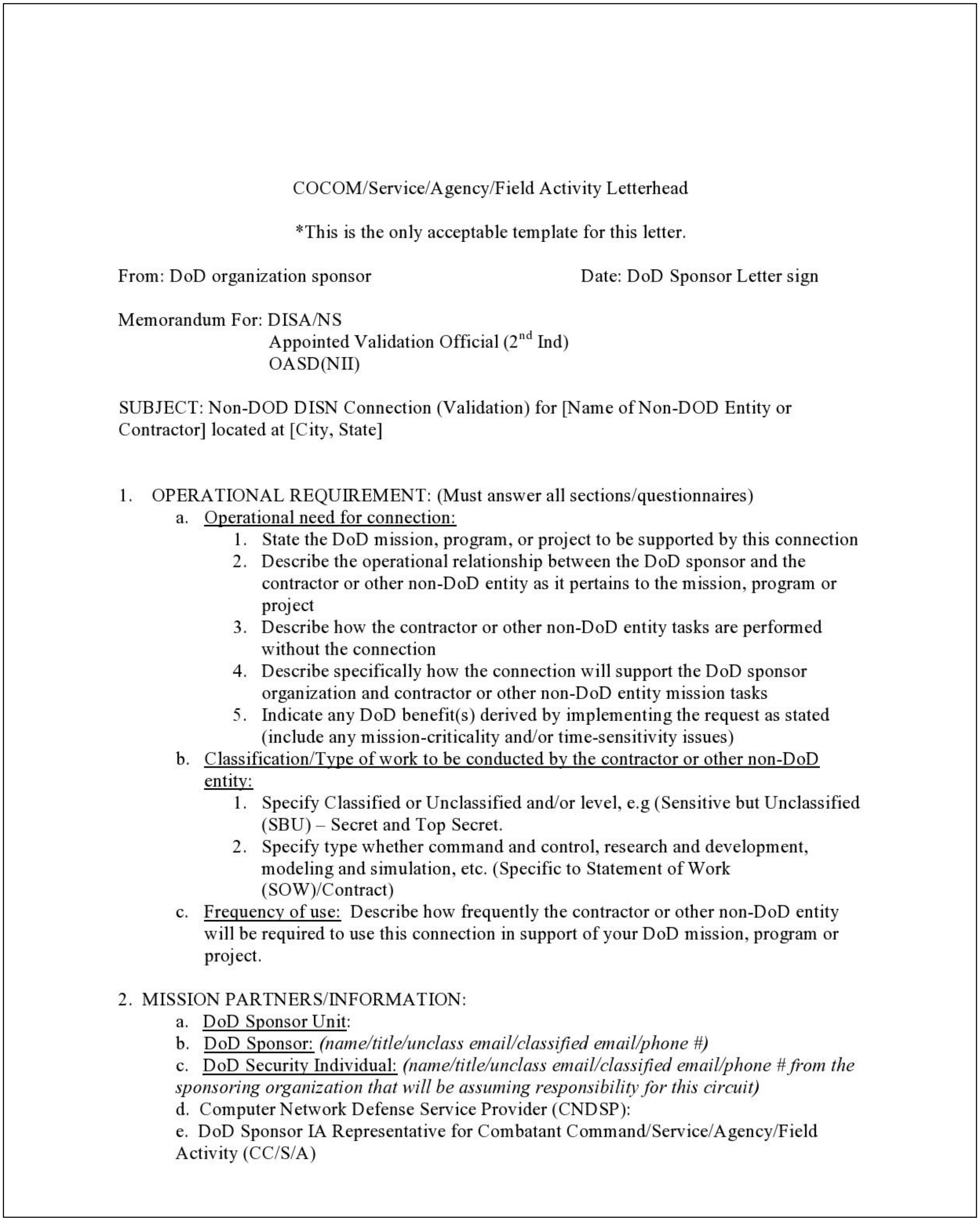
The current version of the template should always be downloaded from the site: http://www.disa.mil/connect/library/index.html.

NOTE: *Validation letters must be revalidated at a minimum of every three years. Validation letters do not extend past the ATO date. A full validation review is required on an existing circuit(s) when any of the following changes/conditions occurs:*

- New Sponsor
- New Contract
- Change of Location
- Change or Expansion of Mission

Revalidation is initiated through the SM’s office (see Appendix B).

Non-DoD DISN Connection Validation Template Sample



COCOM/Service/Agency/Field Activity Letterhead

*This is the only acceptable template for this letter.

From: DoD organization sponsor Date: DoD Sponsor Letter sign

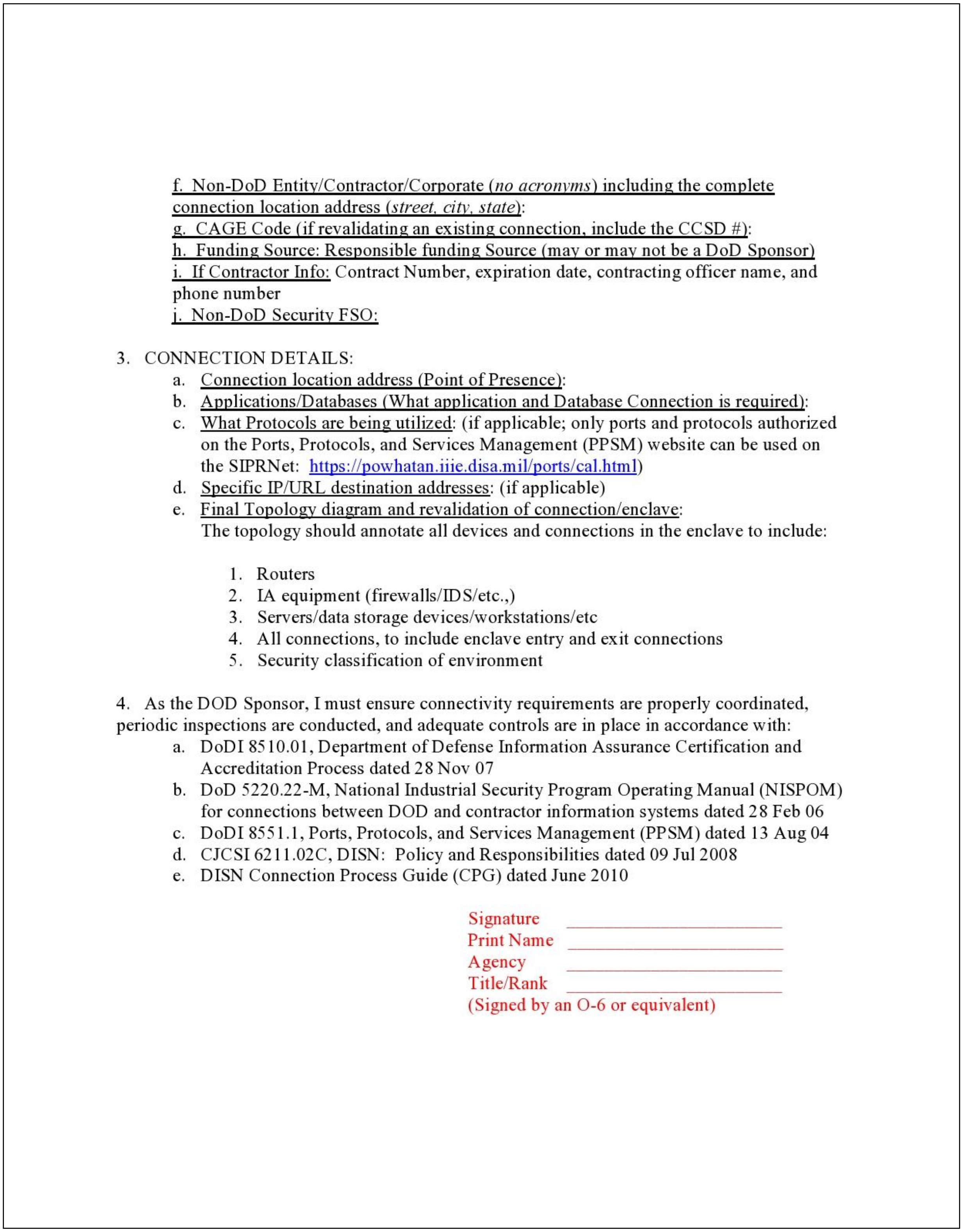
Memorandum For: DISA/NS
Appointed Validation Official (2nd Ind)
OASD(NII)

SUBJECT: Non-DOD DISN Connection (Validation) for [Name of Non-DOD Entity or Contractor] located at [City, State]

1. OPERATIONAL REQUIREMENT: (Must answer all sections/questionnaires)
   a. Operational need for connection:
      1. State the DoD mission, program, or project to be supported by this connection
      2. Describe the operational relationship between the DoD sponsor and the contractor or other non-DoD entity as it pertains to the mission, program or project
      3. Describe how the contractor or other non-DoD entity tasks are performed without the connection
      4. Describe specifically how the connection will support the DoD sponsor organization and contractor or other non-DoD entity mission tasks
      5. Indicate any DoD benefit(s) derived by implementing the request as stated (include any mission-criticality and/or time-sensitivity issues)
   b. Classification/Type of work to be conducted by the contractor or other non-DoD entity:
      1. Specify Classified or Unclassified and/or level, e.g (Sensitive but Unclassified (SBU) – Secret and Top Secret.
      2. Specify type whether command and control, research and development, modeling and simulation, etc. (Specific to Statement of Work (SOW)/Contract)
   c. Frequency of use: Describe how frequently the contractor or other non-DoD entity will be required to use this connection in support of your DoD mission, program or project.

2. MISSION PARTNERS/INFORMATION:
   a. DoD Sponsor Unit:
   b. DoD Sponsor: *(name/title/unclass email/classified email/phone #)*
   c. DoD Security Individual: *(name/title/unclass email/classified email/phone # from the sponsoring organization that will be assuming responsibility for this circuit)*
   d. Computer Network Defense Service Provider (CNDSP):
   e. DoD Sponsor IA Representative for Combatant Command/Service/Agency/Field Activity (CC/S/A)

Figure 4 Non-DoD DISN Connection Validation Template Sample (page 1)



f. Non-DoD Entity/Contractor/Corporate (*no acronyms*) including the complete connection location address (*street, city, state*):
g. CAGE Code (if revalidating an existing connection, include the CCSD #):
h. Funding Source: Responsible funding Source (may or may not be a DoD Sponsor)
i. If Contractor Info: Contract Number, expiration date, contracting officer name, and phone number
j. Non-DoD Security FSO:

3. CONNECTION DETAILS:
   a. Connection location address (Point of Presence):
   b. Applications/Databases (What application and Database Connection is required):
   c. What Protocols are being utilized: (if applicable; only ports and protocols authorized on the Ports, Protocols, and Services Management (PPSM) website can be used on the SIPRNet: https://powhatan.iiie.disa.mil/ports/cal.html)
   d. Specific IP/URL destination addresses: (if applicable)
   e. Final Topology diagram and revalidation of connection/enclave:
   The topology should annotate all devices and connections in the enclave to include:

      1. Routers
      2. IA equipment (firewalls/IDS/etc.,)
      3. Servers/data storage devices/workstations/etc
      4. All connections, to include enclave entry and exit connections
      5. Security classification of environment

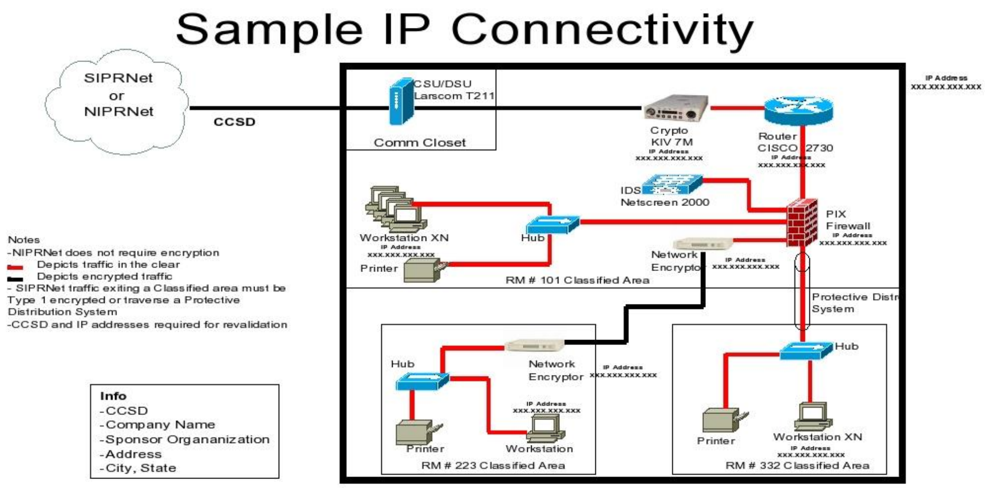
4. As the DOD Sponsor, I must ensure connectivity requirements are properly coordinated, periodic inspections are conducted, and adequate controls are in place in accordance with:
   a. DoDI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process dated 28 Nov 07
   b. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DOD and contractor information systems dated 28 Feb 06
   c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
   d. CJCSI 6211.02C, DISN: Policy and Responsibilities dated 09 Jul 2008
   e. DISN Connection Process Guide (CPG) dated June 2010

Signature ________________________
Print Name ________________________
Agency ________________________
Title/Rank ________________________
(Signed by an O-6 or equivalent)

Figure 5 Non-DoD DISN Connection Validation Template Sample (page 2)

SAMPLE OF AN IT TOPOLOGY DIAGRAM

ILAP Domain Configuration @ ABCDEF Systems



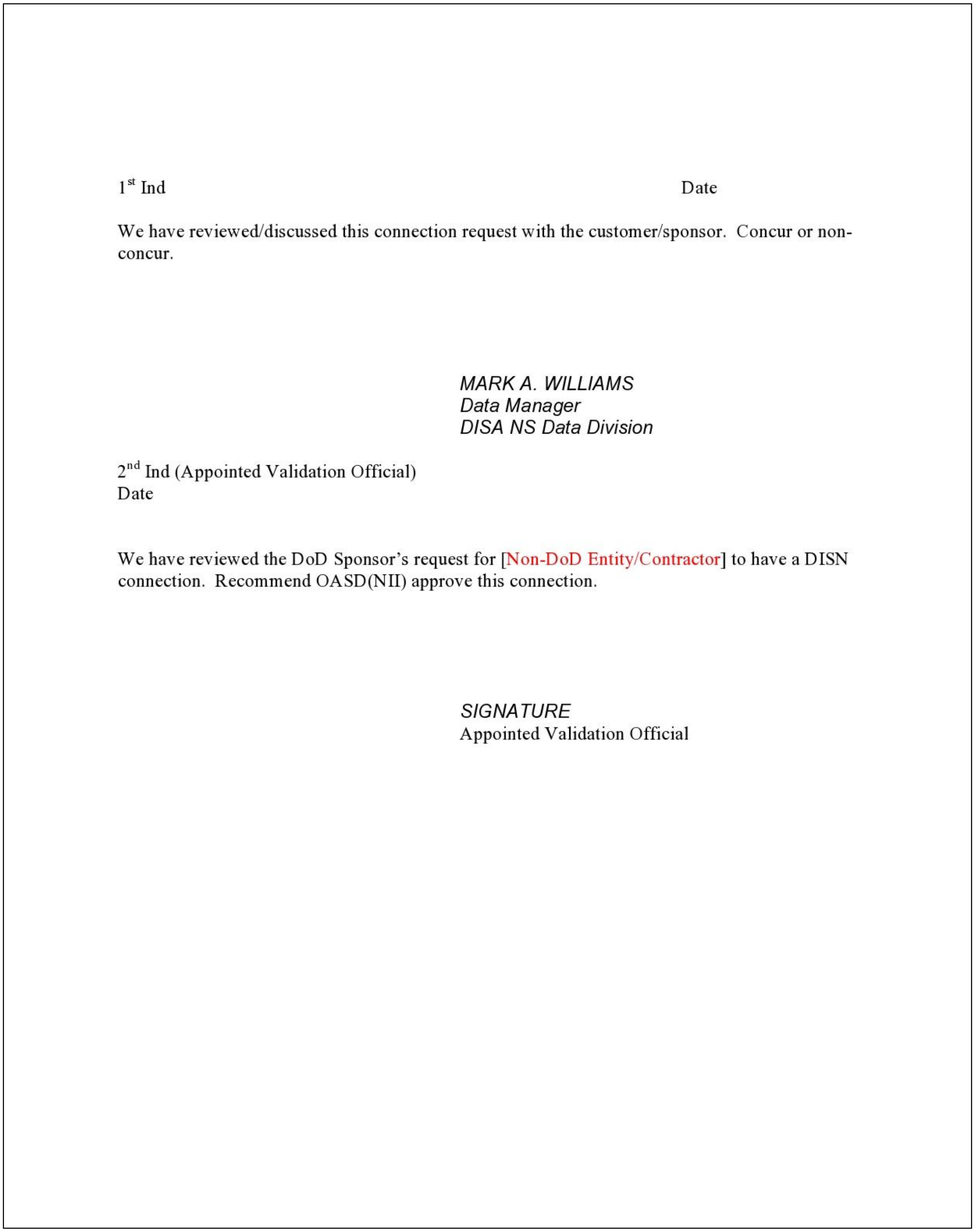
Notes
-NIPRNet does not require encryption
🟥 Depicts traffic in the clear
■ Depicts encrypted traffic
- SIPRNet traffic exiting a Classified area must be Type 1 encrypted or traverse a Protective Distribution System
-CCSD and IP addresses required for revalidation

Info
-CCSD
-Company Name
-Sponsor Organanization
-Address
-City, State

Identify equipment ,(e.g., LARSCOM Access T-1 XXX DSU/CSU,; CISCO WC-1DSU-T1-V2-RF; Cisco 3600 Router; Cisco IDS 4210 Sensor,Cisco 4900 Catalyst Switch) and include all IP addresses, etc.

The letter must include signature pages below. All sections in red must be filled out by the Sponsor. Signatures will be obtained within the respective offices.]

Figure 6 Non-DoD DISN Connection Validation Template Sample (page 3)



1st Ind Date

We have reviewed/discussed this connection request with the customer/sponsor. Concur or non-concur.

MARK A. WILLIAMS
Data Manager
DISA NS Data Division

2nd Ind (Appointed Validation Official)
Date

We have reviewed the DoD Sponsor's request for [Non-DoD Entity/Contractor] to have a DISN connection. Recommend OASD(NII) approve this connection.

SIGNATURE
Appointed Validation Official

Figure 7 Non-DoD DISN Connection Validation Template Sample (page 4)

This page intentionally left blank.

APPENDIX B

NON-DOD DISN CONNECTION REVALIDATION TEMPLATE

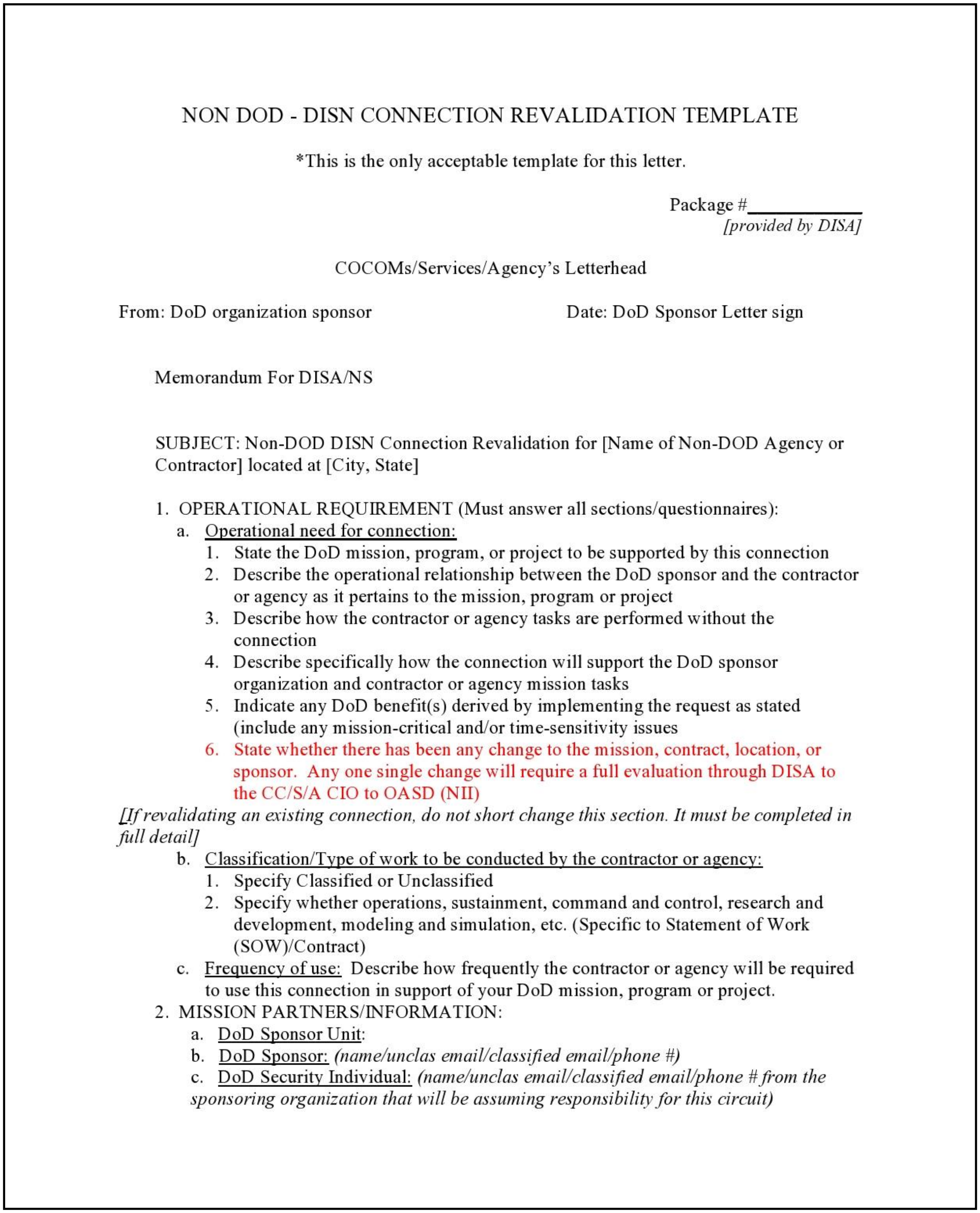
This appendix provides a sample of the template for the Non-DoD DISN Connection Revalidation Letter. This is the only acceptable template for this letter. Once completed, submit the letter according to the instructions identified in Section 3.2.

The current version of the template should always be downloaded from the site: http://www.disa.mil/connect/library/index.html.

A revalidation review is required on an existing circuit(s) when OSD approval has expired and one of the listed changes/conditions below occurs:

- New Sponsor
- New Contract
- Change of Location
- Change/Expansion of Mission

Non-DoD DISN Connection Revalidation Template Sample



NON DOD - DISN CONNECTION REVALIDATION TEMPLATE

*This is the only acceptable template for this letter.

Package #____________
[provided by DISA]

COCOMs/Services/Agency's Letterhead

From: DoD organization sponsor Date: DoD Sponsor Letter sign

Memorandum For DISA/NS

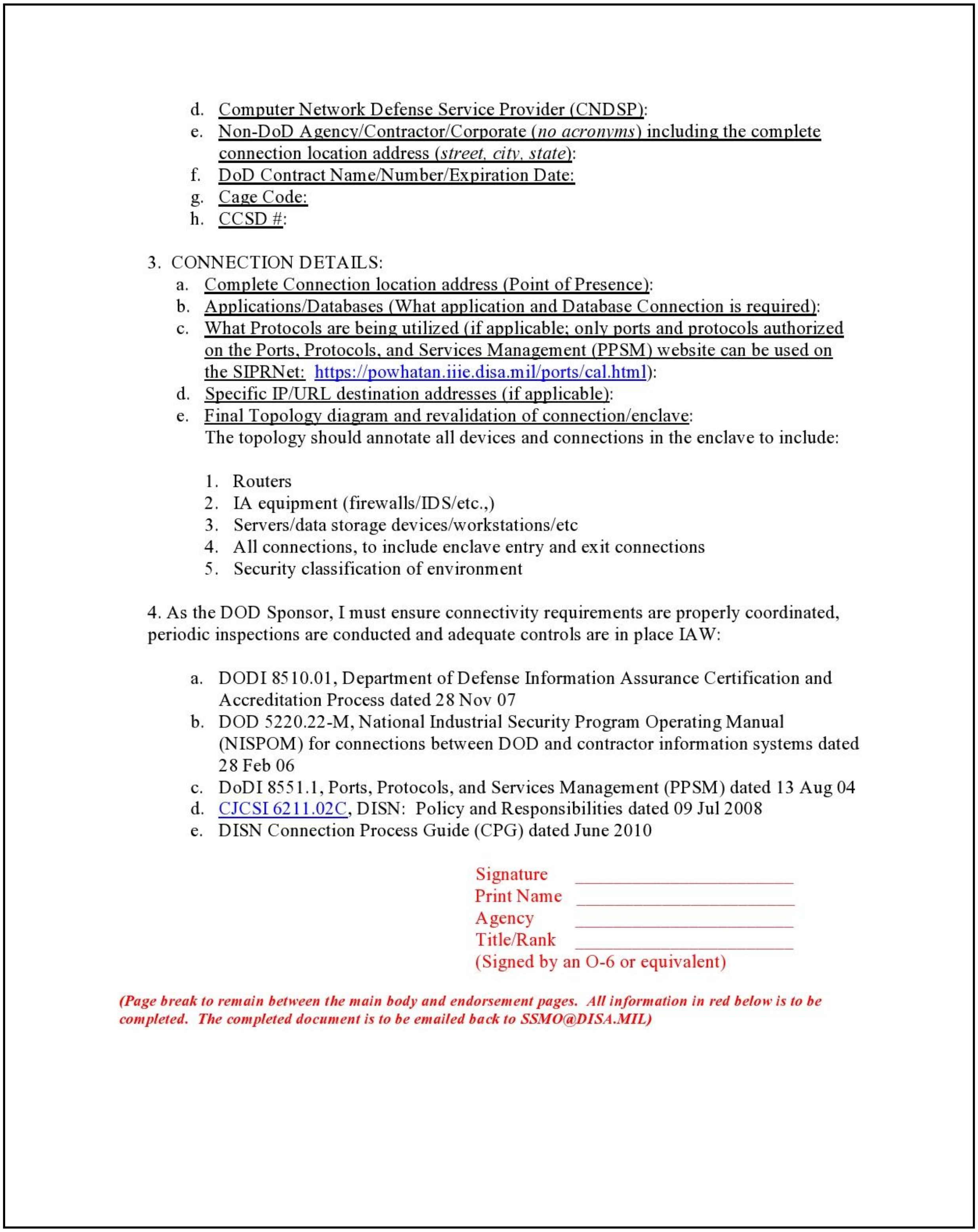
SUBJECT: Non-DOD DISN Connection Revalidation for [Name of Non-DOD Agency or Contractor] located at [City, State]

1. OPERATIONAL REQUIREMENT (Must answer all sections/questionnaires):
   a. Operational need for connection:
      1. State the DoD mission, program, or project to be supported by this connection
      2. Describe the operational relationship between the DoD sponsor and the contractor or agency as it pertains to the mission, program or project
      3. Describe how the contractor or agency tasks are performed without the connection
      4. Describe specifically how the connection will support the DoD sponsor organization and contractor or agency mission tasks
      5. Indicate any DoD benefit(s) derived by implementing the request as stated (include any mission-critical and/or time-sensitivity issues
      6. State whether there has been any change to the mission, contract, location, or sponsor. Any one single change will require a full evaluation through DISA to the CC/S/A CIO to OASD (NII)

[If revalidating an existing connection, do not short change this section. It must be completed in full detail]

   b. Classification/Type of work to be conducted by the contractor or agency:
      1. Specify Classified or Unclassified
      2. Specify whether operations, sustainment, command and control, research and development, modeling and simulation, etc. (Specific to Statement of Work (SOW)/Contract)
   c. Frequency of use: Describe how frequently the contractor or agency will be required to use this connection in support of your DoD mission, program or project.
2. MISSION PARTNERS/INFORMATION:
   a. DoD Sponsor Unit:
   b. DoD Sponsor: *(name/unclas email/classified email/phone #)*
   c. DoD Security Individual: *(name/unclas email/classified email/phone # from the sponsoring organization that will be assuming responsibility for this circuit)*

Figure 8 Non-DoD DISN Connection Revalidation Template Sample (page 1)



d. Computer Network Defense Service Provider (CNDSP):
e. Non-DoD Agency/Contractor/Corporate (*no acronyms*) including the complete connection location address (*street, city, state*):
f. DoD Contract Name/Number/Expiration Date:
g. Cage Code:
h. CCSD #:

3. CONNECTION DETAILS:

a. Complete Connection location address (Point of Presence):
b. Applications/Databases (What application and Database Connection is required):
c. What Protocols are being utilized (if applicable; only ports and protocols authorized on the Ports, Protocols, and Services Management (PPSM) website can be used on the SIPRNet: https://powhatan.iiie.disa.mil/ports/cal.html):
d. Specific IP/URL destination addresses (if applicable):
e. Final Topology diagram and revalidation of connection/enclave:
The topology should annotate all devices and connections in the enclave to include:

1. Routers
2. IA equipment (firewalls/IDS/etc.,)
3. Servers/data storage devices/workstations/etc
4. All connections, to include enclave entry and exit connections
5. Security classification of environment

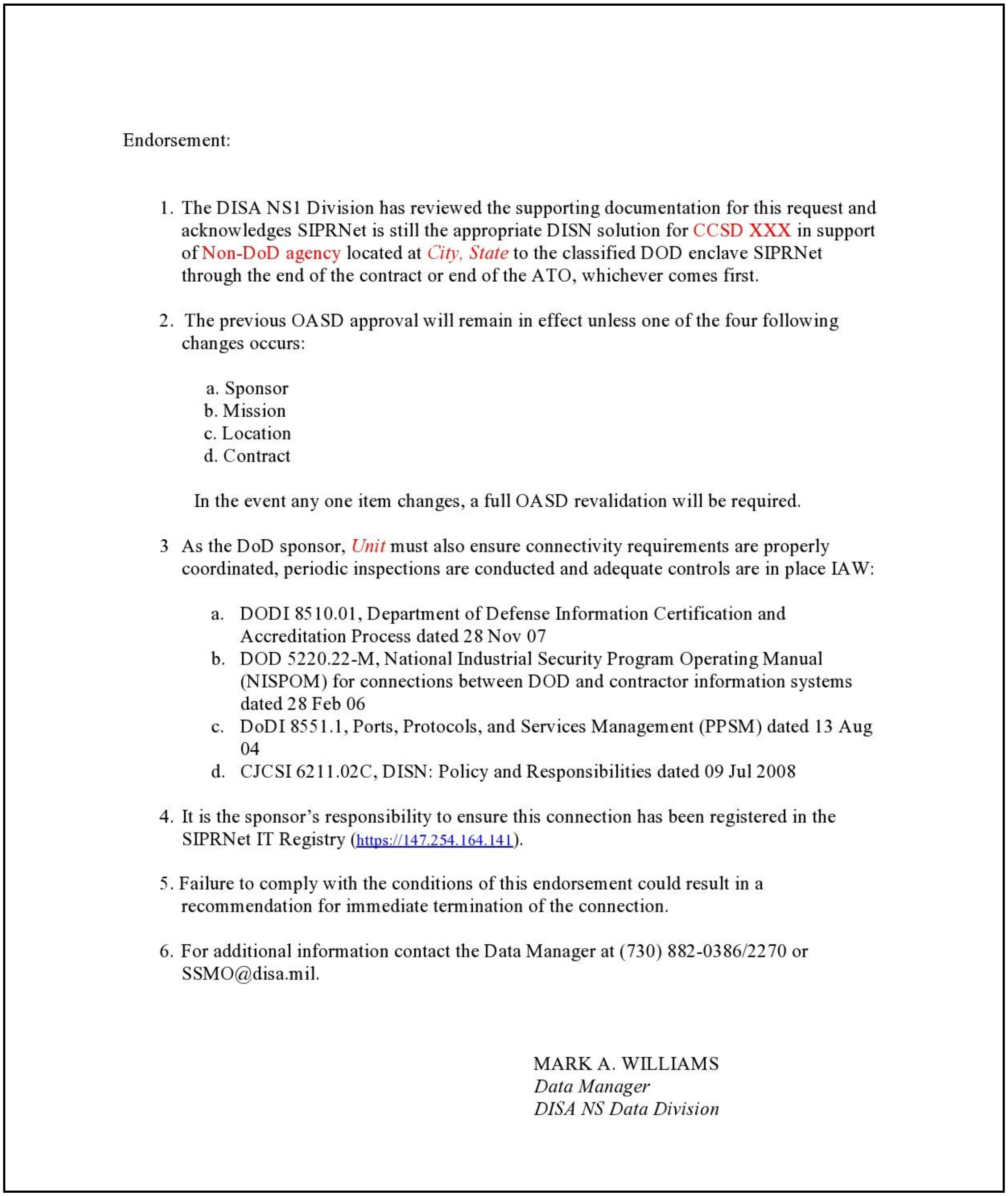
4. As the DOD Sponsor, I must ensure connectivity requirements are properly coordinated, periodic inspections are conducted and adequate controls are in place IAW:

a. DODI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process dated 28 Nov 07
b. DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DOD and contractor information systems dated 28 Feb 06
c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
d. CJCSI 6211.02C, DISN: Policy and Responsibilities dated 09 Jul 2008
e. DISN Connection Process Guide (CPG) dated June 2010

Signature ________________________
Print Name ________________________
Agency ________________________
Title/Rank ________________________
(Signed by an O-6 or equivalent)

(Page break to remain between the main body and endorsement pages. All information in red below is to be completed. The completed document is to be emailed back to SSMO@DISA.MIL)

Figure 9 Non-DoD DISN Connection Revalidation Template Sample (page 2)



Endorsement:

1. The DISA NS1 Division has reviewed the supporting documentation for this request and acknowledges SIPRNet is still the appropriate DISN solution for CCSD XXX in support of Non-DoD agency located at *City, State* to the classified DOD enclave SIPRNet through the end of the contract or end of the ATO, whichever comes first.

2. The previous OASD approval will remain in effect unless one of the four following changes occurs:

   a. Sponsor
   b. Mission
   c. Location
   d. Contract

   In the event any one item changes, a full OASD revalidation will be required.

3 As the DoD sponsor, *Unit* must also ensure connectivity requirements are properly coordinated, periodic inspections are conducted and adequate controls are in place IAW:

   a. DODI 8510.01, Department of Defense Information Certification and Accreditation Process dated 28 Nov 07
   b. DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DOD and contractor information systems dated 28 Feb 06
   c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
   d. CJCSI 6211.02C, DISN: Policy and Responsibilities dated 09 Jul 2008

4. It is the sponsor's responsibility to ensure this connection has been registered in the SIPRNet IT Registry (https://147.254.164.141).

5. Failure to comply with the conditions of this endorsement could result in a recommendation for immediate termination of the connection.

6. For additional information contact the Data Manager at (730) 882-0386/2270 or SSMO@disa.mil.

MARK A. WILLIAMS
Data Manager
DISA NS Data Division

Figure 10 Non-DoD DISN Connection Revalidation Template Sample (page 3)

APPENDIX C

DRSN – CLASSIFIED

This appendix provides the necessary steps and information for a Defense Red Switched Network (DRSN) connection. It is intended to supplement the detailed information provided in Section 3, of this guide with DRSN-specific information. Any deviations from those steps or additional requirements are identified in this appendix.

C.1 DRSN Connection Process

DRSN service requests must be defined, validated, coordinated, and approved through DISA Single System Manager (SSM). Requests should be validated by the appropriate CC/S/A/FA. These actions should be approved prior to forwarding to DISA for coordination and implementation.

Per DoDI 8100.04, connection to the DRSN requires purchase of voice equipment that is identified on the UC Approved Products List (APL). All items on the APL require certification and accreditation for interoperability (IO) and IA. Requests for an interim certificate to operate (ICTO) should be forwarded to the CJCS for consideration.

For information on APL approved products and the APL process for getting equipment added to that list, refer to the link: http://jitc.fhu.disa.mil/apl/drsn.html.

Follow Steps 1-12 in the Section 3 of this guide.

C.2 Process Deviations and/or Additional Requirements

These procedures apply to the Joint Staff, Combatant Commands (COCOMs), Services, and Defense agencies. All DRSN switch connection requests must be forwarded through the requestor's chain of command to the appropriate approval authority. Non-DoD agency requests must be sponsored by a DoD component and forwarded through the Joint Staff to the OASD(NII)/DoD CIO for final approval.

C.3 DRSN Connection Process Checklist

The checklist below provides the key activities that are performed by assigned organizations during the DRSN connection approval process.

Item	Connection Process	Action
1	User prepares DRSN service request IAW CJCSI 6215.01C and submits to JS/J6C	Authorized User
2	JS/J6C receives user CJCSI 6215.01C DRSN request	JS/J6C
3	JS/J6C reviews and validates user's request	JS/J6C
4	JS/J6C sends user's request to DISA/NS41 for Technical/Engineering service installation	DISA/NS41
5	DISA/NS41 conducts Technical/Engineering review at the user's sites	DISA/NS41
6	DISA/NS41 enters request into the CJCSI 6215.01C database record log	DISA/NS41
7	DISA/NS41 submits Technical/Engineering review results to JS/J6C	DISA/NS41
8	JS/J6C approval process occurs	JS/J6C

Item	Connection Process	Action
9	DISA/NS41 updates CJCSI 6215.01C database with results and posts to the DRSN DKO-S website	DISA/NS41
10	To obtain the DKO-S link to view request status, contact Secure Voice Services at the email or phone numbers listed below. General information can be viewed on the DKO link below: https://www.us.army.mil/suite/page/547539	Authorized User

Table 2 DRSN Connection Process Checklist

C.4 Points of Contact

Secure Voice Services	
Unclassified email	hostmaster@nic.mil
Phone (Commercial)	703-882-0318/0322/0102/0330
Phone (DSN)	312-381-0318

C.5 Additional Policy and Guidance Documents

DoDI 4630.8	*Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004 (ref r)
CJCSI 6212.01E	*Interoperability and Supportability of Information Technology and National Security Systems*, 15 December 2008 (ref i)
CJCSI 6215.01C	*Policy For Department Of Defense Voice Networks With Real Time Services (RTS)*, 9 November 2007 (ref b)
DoDI 8100.4	*Department of Defense Instruction (DoDI) DoD Unified Capabilities (UC)*, 9 December 2010 (ref o)
DoDI 8510.01	*DoD Information Assurance Certification and Accreditation Process*, 28 November 2007 (ref g)
ICD 503	*Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation*, 15 September 2008 (ref s)

C.6 Sample Topology Diagrams

Contact Secure Voice Services for technical guidance on proposed network topology at the contact numbers listed in the Points of Contact above.

APPENDIX D

DSN – UNCLASSIFIED

This appendix provides the necessary steps and information to process a Defense Switched Network (DSN) telecommunication switch connection. It is intended to supplement the detailed information provided in Section 3 of this guide with DSN-specific information. Any deviations from those steps or additional requirements are identified in this appendix.

D.1 DSN Connection Process

Follow steps 1-12 in Section 3 of this guide.

D.2 Process Deviations and/or Additional Requirements

Per DoDI 8100.4 (ref o), connection of an applicable telecommunication switch to the DSN requires procurement of interfacing hardware and/or software components that are identified on the DoD UC Approved Products List (APL). All items on the APL require certification and accreditation IO and IA. If the intended product is not on the APL, it will either need to be JITC IO and IA tested, certified, and placed on the APL, or authorized for purchase via OASD(NII) policy waiver before the product can be purchased and connected to the DISN.

For information on APL products and the APL process for getting equipment added to that list, refer to the links below:

- DSN/DoD UC APL pages: https://aplits.disa.mil/processAPList.do
- UC Testing and Certification: http://www.disa.mil/ucco/index.html
- DSN Services and Capabilities: http://www.disa.mil/dsn/index.html

D.3 DSN Connection Process Checklist

This checklist provides the key activities that must be performed by the customer/sponsor during the DSN connection approval process.

Item	DoD Customer		Non-DoD Customer	
	New	Existing	New	Existing
Obtain OSD approval for non-DoD connection			√	√[1]
Obtain APL approval for voice equipment not currently on the APL list	√		√	
Provision the connection	√		√	√[1]
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO)	√	√	√	√
Register the connection	√	√[2]	√	√[1]
Register in the SNAP database	√	√[2]	√	√[1]
Register in the PPSM database	√	√[2]	√	√[1]
Register in the DITPR database	√	√[2]	√	√[1]
Complete the CAP package	√	√	√	√
DIACAP Executive Package (or equivalent)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile (include switching equipment—i.e., vendor model and software)	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
DAA Appointment current in database	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
Proof of Contract			√	√
OASD(NII) Approval Letter			√	√
Complete ATC submittal form (see 1.4)	√	√	√	√
Submit the CAP package to the CAO	√	√	√	√
Receive DSN ATC/IATC	√	√	√	√

Table 3 DSN Connection Process Checklist

[1] This step is not required for existing non-DoD customer connections unless there has been a change in sponsor, mission requirement, contract, or location, or the connection has not been registered.

[2] This step is not required for existing connections that are already registered and where all information is current.

D.4 Points of Contact

Unified Capabilities Certification Office (UCCO)	
Unclassified email	UCCO@disa.mil

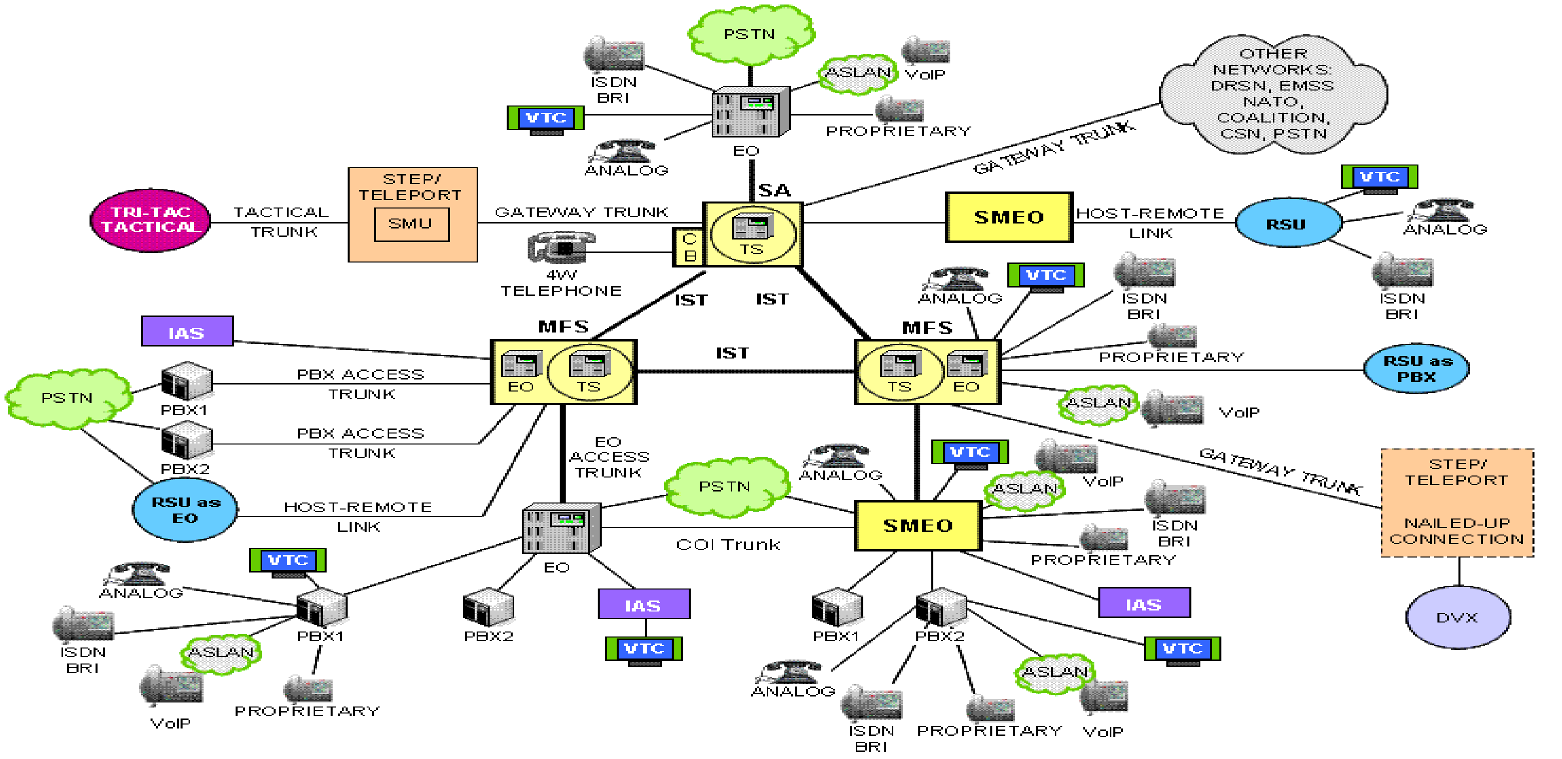
Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Unclassified email	UCAO@disa.mil	UCAO@disa.mil
Phone (Commercial)	703-882-2086	703-882-2086, 301-225-2900/2901
Phone (DSN)	312-381-2086	312-381-2086, 312-761-2900/2901
Fax (Commercial)	703-882-2813	703-882-2813
Fax (DSN)	312-381-2813	312-381-2813

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Classified email	DGSC@cols.disa.smil.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

D.5 Additional Policy and Guidance Documents

DSN ATC Request Submittal Form	http://www.disa.mil/dsn/jic/atcsubmittal.html
DoDI 8100.4	*Department of Defense Instruction (DoDI) DoD Unified Capabilities (UC)*, 9 December 2010 (ref o)
CJCSI 6215.01C	*Policy For Department Of Defense Voice Networks With Real Time Services (RTS)*, 9 November 2007 (ref b)

D.6 Sample Topology Diagrams (with and without VOIP)



LEGEND:

4W	4-Wire Subscriber Line
BRI	Basic Rate Interface
CB	Channel Bank
COI	Community of Interest
CSN	Canadian Switched Network
DRSN	Defense RED Switch Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
MFS	Multifunction Switch
MLPP	Multilevel Precedence and Preemption
NATO	North American Treaty Organization
PBX1	Private Branch Exchange (MLPP Capable)
PBX2	Private Branch Exchange (Non-MLPP Capable)
PSTN	Public Switching Telephone Network
RSU	Remote Switching Unit
SA	Stand-Alone Switch
SMEO	Small End Office
SMU	Switch Multiplex Unit
STEP	Standard Tactical Entry Point
Tri-Tac	Tri-Service Tactical
TS	Tandem Switch
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing

Figure 11 Sample DSN Topology with and without VOIP

D.7 Example Installation Configurations

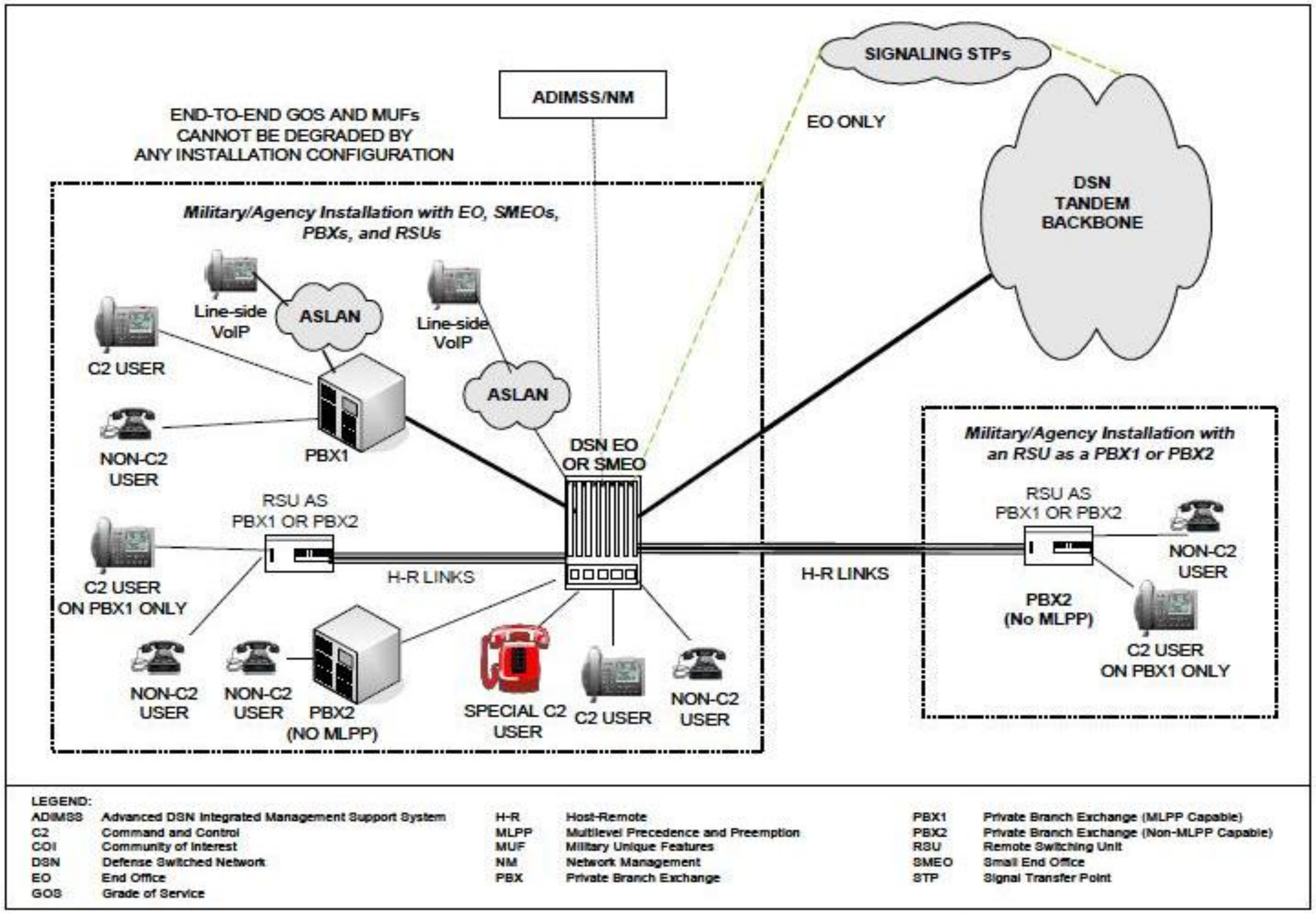

SIGNALING STPs
ADIMSS/NM
END-TO-END GOS AND MUFs CANNOT BE DEGRADED BY ANY INSTALLATION CONFIGURATION
EO ONLY
DSN TANDEM BACKBONE
Military/Agency Installation with EO, SMEOs, PBXs, and RSUs
Line-side VoIP
ASLAN
Line-side VoIP
C2 USER
ASLAN
NON-C2 USER
PBX1
DSN EO OR SMEO
RSU AS PBX1 OR PBX2
C2 USER ON PBX1 ONLY
H-R LINKS
NON-C2 USER
NON-C2 USER
PBX2 (NO MLPP)
SPECIAL C2 USER
C2 USER
NON-C2 USER
H-R LINKS
Military/Agency Installation with an RSU as a PBX1 or PBX2
RSU AS PBX1 OR PBX2
NON-C2 USER
PBX2 (No MLPP)
C2 USER ON PBX1 ONLY
LEGEND:
ADIMSS Advanced DSN Integrated Management Support System
C2 Command and Control
COI Community of Interest
DSN Defense Switched Network
EO End Office
GOS Grade of Service
H-R Host-Remote
MLPP Multilevel Precedence and Preemption
MUF Military Unique Features
NM Network Management
PBX Private Branch Exchange
PBX1 Private Branch Exchange (MLPP Capable)
PBX2 Private Branch Exchange (Non-MLPP Capable)
RSU Remote Switching Unit
SMEO Small End Office
STP Signal Transfer Point

Figure 12 Example Installation Configurations

This page intentionally left blank.

APPENDIX E

DISN-LES – CLASSIFIED

This appendix provides the necessary steps and information for a DISN Leading Edge Services (DISN-LES) connection. It is intended to supplement the detailed information provided in Section 3 of this guide with DISN-LES specific information. Any deviations from those steps or additional requirements are identified in this appendix.

E.1 DISN-LES Connection Process

Follow steps 1-12 in Section 3 of this guide.

E.2 Process Deviations and/or Additional Requirements

Step 8 DoD Contractor connections must go through the Defense Security Service (DSS) for accreditation of their facilities. This includes direct connections to the DISN-LES. For questions regarding DSS accreditation, contact the DSS SIPRNet Program Management Office at disn@dss.mil or by phone at 888-282-7682, Option 2.

Step 10 All DoD and non-DoD customers/sponsors must complete the DISN-LES Customer Questionnaire (DCQ) and submit it with the CAP package. The DCQ must be signed by the connection/enclave DAA. The DCQ is available on the DISN connection process webpage at http://www.disa.mil/connect/classified/dod_exist_les.html.

- All 'Yes' responses must be explained
- All POC information must be completed for the questionnaire to be accepted by the CAO

E.3 DISN-LES Connection Process Checklist

This checklist provides the key activities that must be performed by the customer/sponsor during the DISN-LES connection approval process.

Item	DoD Customer		Non-DoD Customer	
	New	Existing	New	Existing
Obtain OSD approval for non-DoD connection			√	√[3]
Provision the connection	√		√	√[3]
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO)	√	√	√	√
Register the connection[4]	√		√	√[3]
Register in the GIAP/SGS database	√		√	√[3]
Register in the PPSM database	√		√	√[3]
Register in the SIPRNet IT Registry database	√		√	√[3]
Complete the CAP package	√	√	√	√
DIACAP Executive Package (or equivalent for non-DoD entities)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
DAA Appointment Letter	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
DISN-LES Customer Questionnaire	√	√	√	√
Proof of Contract			√	√
OASD(NII) Approval Letter			√	√
Submit the CAP package to the CAO	√	√	√	√
Receive DISN-LES ATC/IATC	√	√	√	√

Table 4 DISN-LES Connection Process Checklist

[3] This step is not required for existing non-DoD customer connections unless there has been a change in sponsor, mission requirement, contract, or location.

[4] For non-Zone C requests.

E.4 Points of Contact

DISN-LES Service Manager - General	
Unclassified email	disnles@disa.mil
Phone (Commercial)	301-225-2463
Phone (DSN)	312-761-2463

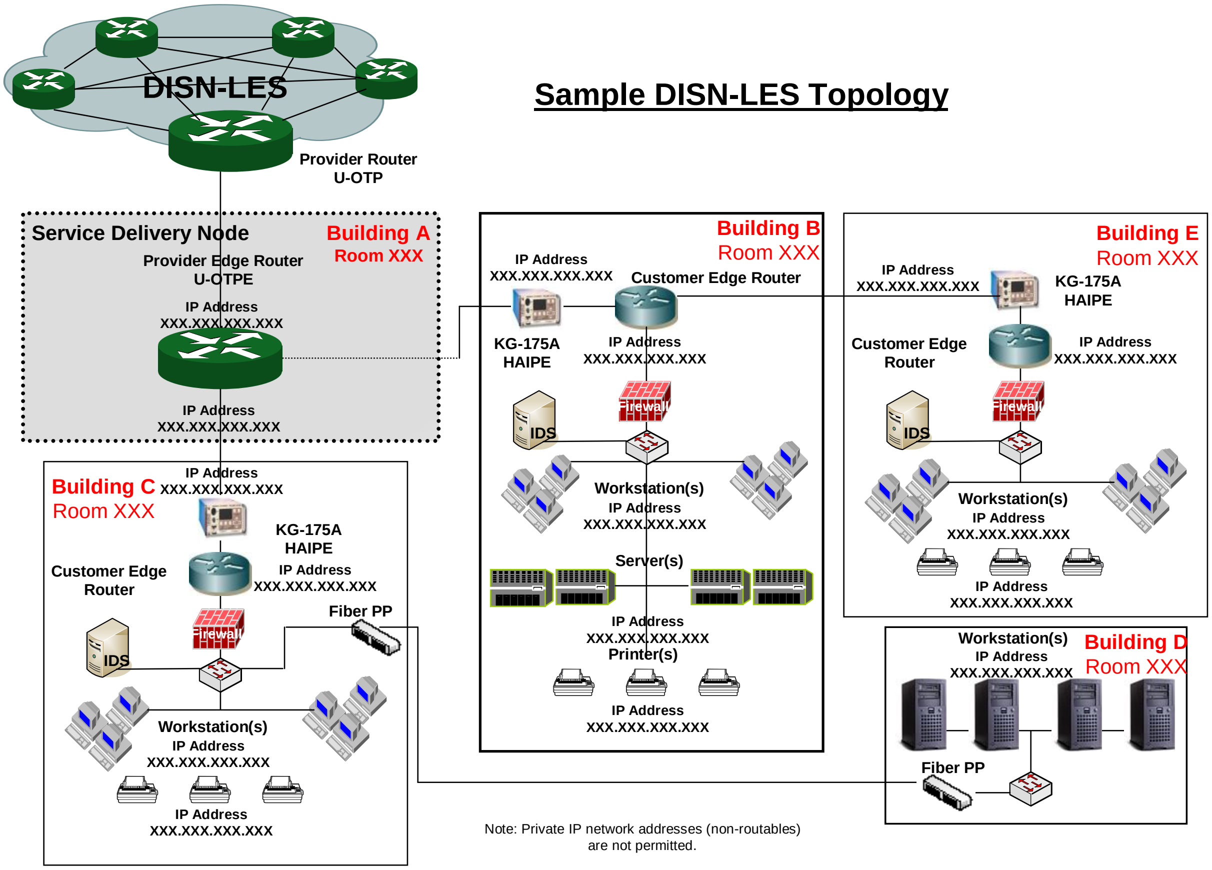
DISN-LES Service Manager - Technical	
Unclassified email	disnles@disa.mil
Phone (Commercial)	301-225-2054
Phone (DSN)	312-761-2054

Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Unclassified email	CCAO@disa.mil	CCAO@disa.mil
Phone (Commercial)	703-882-1455	703-882-1455, 301-225-2900/2901
Phone (DSN)	312-381-1455	312-381-1455, 312-761-2900/2901
Fax (Commercial)	703-882-2813	703-882-2813
Fax (DSN)	312-381-2813	312-381-2813

E.5 Sample Topology Diagrams

All topologies must include:

- Topology date
- CCSD (preferably near premise router)
- IP addresses for all devices within the enclave, and the following devices must include additional information specific to them:
- Firewalls: manufacturer, model, and software/firmware version
- IDS: manufacturer, model, and software/firmware version
- Servers: server function (i.e., Outlook Web Access (OWA), Web Server, etc.) and operating system (including most updated Service Pack installed on system)
- Workstations: operating system (including most updated Service Pack installed on system)



Note: Private IP network addresses (non-routables) are not permitted.

Figure 13 Sample DISN-LES Topology

APPENDIX F

DVS – CLASSIFIED AND UNCLASSIFIED

This appendix provides the necessary steps and information for a DISN Video Services (DVS) connection. It is intended to supplement the detailed information provided in Section 3 of this guide with DVS-specific information. Any deviations from those steps or additional requirements are identified in this appendix.

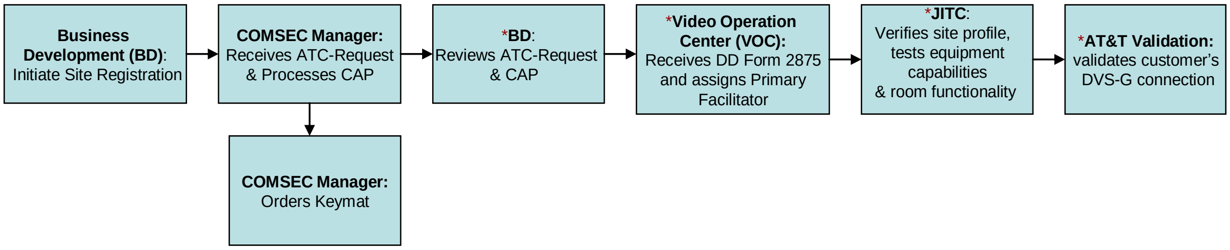
F.1 DVS Connection Process

To obtain DVS service, the customer/sponsor must have an existing commercial Integrated Services Digital Network (ISDN) service and/or order a DISN transmission path (DSN, Commercial, or Federal Telecommunications Service (FTS)). Information on ordering each of these services is provided in the service's appendix to this guide. Once the transmission path is obtained and corresponding ATC/IATC is granted, the customer/sponsor can then proceed with ordering the DVS service.

F.2 Process Deviations and/or Additional Requirements

Until additional hub resources are available, DVS-G registrations within CONUS will be limited only to those prospective sites with an urgent valid requirement. Unless urgent, no new site registrations are being accepted. When required, DVS can facilitate "new" critical and/or urgent requirements on a case-by-case basis. Please contact the DGSC - DVS with the specifics of your request.

DVS-G Registration Process


Business Development (BD): Initiate Site Registration
COMSEC Manager: Receives ATC-Request & Processes CAP
COMSEC Manager: Orders Keymat
***BD**: Reviews ATC-Request & CAP
***Video Operation Center (VOC):** Receives DD Form 2875 and assigns Primary Facilitator
***JITC**: Verifies site profile, tests equipment capabilities & room functionality
***AT&T Validation:** validates customer's DVS-G connection

(*) Site will receive automated email informing them to proceed to next step in registration process

Figure 14 DVS-G Registration Process

F.3 DVS Connection Process Checklist

Item	DoD Customer		Non-DoD Customer	
	New	Existing	New	Existing
Obtain OSD approval for non-DoD connection			√	
Register the connection	√	√	√	√
Register in the DISN Video Services – Web Site (DVS-WS) database	√	√	√	√
Complete the CAP package (Classified: up to and including SECRET)	√	√	√	√
Access Approval Document	√	√	√	√
Authorization to Operate	√	√	√	√
Topology Diagram	√	√	√	√
Copy of Transport (DSN) ATC	√	√	√	√
DAA Appointment Letter (If DAA is not SES or GO)	√	√	√	√
Complete the CAP package (Unclassified sites)	√	√	√	√
Authority To Connect Request	√	√	√	√
Copy of Transport (DSN) ATC	√	√	√	√
Topology diagram	√	√	√	√
Designate primary facilitation	√	√	√	√
Complete DD Form 2875	√	√	√	√
Complete JITC verification	√	√	√	√
Complete AT&T validation	√	√	√	√

Table 5 DVS Checklist

Step 1 Complete Initial Registration with Business Development (BD)

- BD answers all questions, acts as primary POC to the customer through the registration process, and refers them to the DVS-WS website http://www.disa.mil/disnvtc/become.htm to complete all required documents
- Upon online registration, customer provides required information; BD will assist the customer in completing this process as necessary
- BD then reviews the completed Site Profile, assigns a site ID and "Submits pending site" via DVS-WS
- After the site ID is assigned, BD tracks the process using DVS-WS "New Site Registration Queue"

Step 2 Submit CAP Documents to Communications Security (COMSEC) Manager

- Classified (up to and including SECRET) Sites: Customer completes an ATO and an Access Approval Document (AAD) (with DAA signatures) and submits them with a suite configuration drawing and a copy of the transport (DSN) ATC to the DVS COMSEC Manager for approval. Classified customers should allow 2-4 weeks to receive the COMSEC Keymat from the National Security Agency (NSA). Contact the CAD to register new transports (see POC information in F.4).
- Unclassified Sites: Customer completes ATC request with DAA signature (or the signature of a DAA designee) and submits it with a configuration drawing and a copy of the transport (i.e., DSN) ATC to the DVS COMSEC Manager. Contact the CAD to register new transports.
- COMSEC Manager reviews/approves all documents.

NOTE: *If connection is Classified, COMSEC Manager orders KEYMAT and checks the "Crypto approved" column in DVS-WS Site Registration Queue.*

Step 3 Business Development Will Review Site Information

- Reviews Site Profile information for any changes made since initial registration
- After the review is completed, BD checks "BD Approved" column in the DVS-WS New Site Registration Queue

Step 4 Designate Primary Facilitator with the Video Operations Center (VOC)

- Customer completes and submits a signed System Authorization Access Request (DD Form 2875) to the VOC designating a Primary Facilitator for the site (see POC information in F.4)
- VOC processes DD Form 2875 and checks the "PF Assigned" column in DVS-WS New Site Registration Queue

NOTE: *An automated DVS-WS generated email is subsequently sent to the customers advising them to contact JITC to schedule Verification Test.*

Step 5 Complete JITC Site Profile and Equipment/Facility Verification

- JITC verifies customer's site profile information and tests their equipment capabilities and room functionality. Classified customers must have already received an Over The Air Rekey (OTAR) from the VOC before performing the verification test
- Upon successful completion, JITC checks the "JITC Approved" column in the DVS-WS New Site Registration Queue

NOTE: *An automated DVS-WS generated email is subsequently sent to customers advising them to contact AT&T to schedule a Validation Test.*

Step 6 Complete AT&T Validation

- AT&T validates customers can connect to DVS-G as indicated on their site profile
- Upon successful completion, AT&T checks "AT&T Approved" column in the DVS-WS New Site Registration Queue

NOTE: *An automated DVS-WS generated email is subsequently sent to customers advising them that the process is completed and that they can now schedule VTCs on DVS-G.*

F.4 Points of Contact

DVS Connection Process POCs **CONUS (Continental United States), DISA NS5**	
Unclassified email	dccc_dvs@csd.disa.mil
Phone (Commercial)	800-554-DISN (3476)
Phone (DSN)	312-850-4790
Fax (Commercial)	703-681-3826
Fax (DSN)	312-761-3826

DVS Connection Process POCs **Europe, DISA EU52**	
Unclassified email	vtcopseur@disa.mil
Phone (Commercial)	011-49-711-68639-5260/5840/5445
Phone (DSN)	314-434-5260/5840/5445
Fax (Commercial)	011-49-711-68639-5312
Fax (DSN)	314-434-5312

DVS Connection Process POCs **Pacific, DISA PC54**	
Unclassified email	vtcopspac@disa.mil
Phone (Commercial)	808-656-0585
Phone (DSN)	315-456-0585
Fax (Commercial)	808-656-3838
Fax (DSN)	315-456-3838

DVS Connection Process POCs **Southwest Asia (SWA), DISA NS5**	
Unclassified email	vtcops@disa.mil
Phone (Commercial)	703-681-4111
Phone (DSN)	312-761-4111
Fax (Commercial)	703-681-3826
Fax (DSN)	312-761-3826

DVS Connection Process POCs DVS COMSEC Manager	
Unclassified email	DVSTierIII@disa.mil
Phone (Commercial)	703-681-4108
Phone (DSN)	312-761-4108
Fax (Commercial)	703-681-3826
Fax (DSN)	312-761-3826

FSO POC for Circuit and CNDSP Inquiries	
Contact Name	Robert Mawhinney, Chief CNDSP & Planning Branch
Unclassified email	robert.mawhinney@disa.mil
Phone (Commercial)	717-267-9715
Phone (DSN)	312-570-9715

Designate Primary Facilitator with the VOC	
Unclassified email	VOC@disa.mil
Phone (Commercial)	618-220-8688
Phone (DSN)	312-770-8688

AT&T Validation Test	
Phone (Commercial)	800-367-8722
Phone (DSN)	312-533-3000

JITC Certification Test	
Phone (DSN)	312-821-9333

DISN Global Support Center (DGSC)	
Unclassified email	dccc_dvs@csd.disa.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

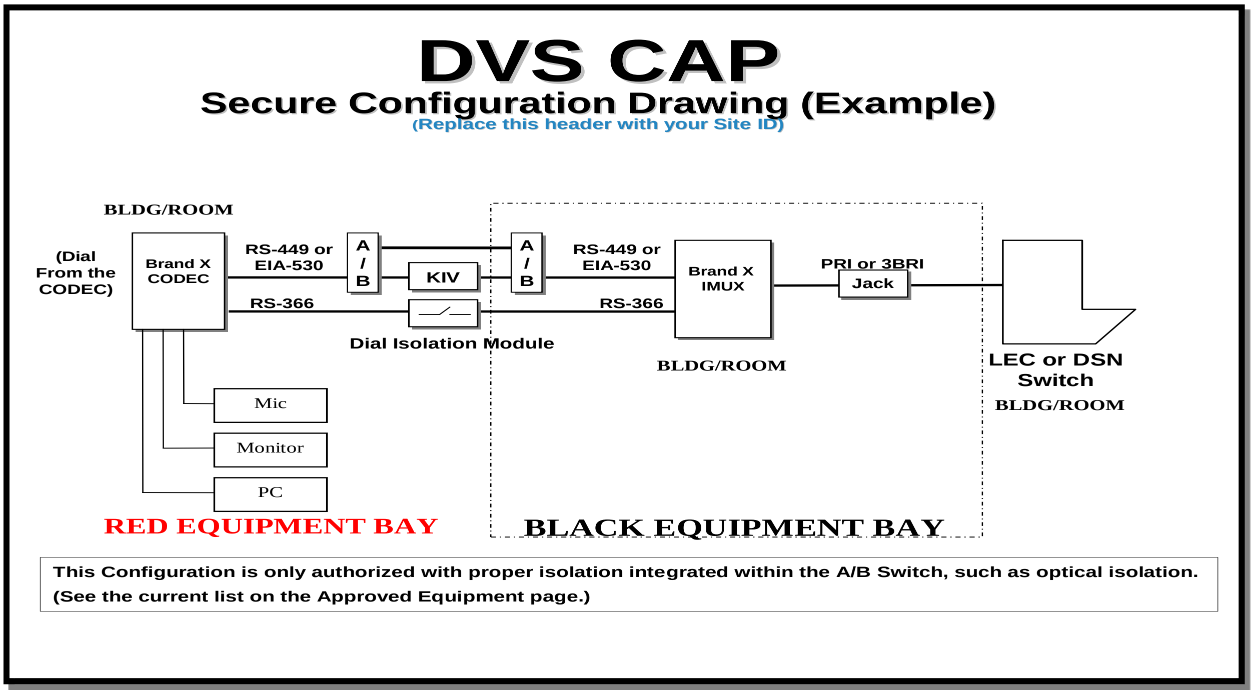
F.5 Additional Policy and Guidance Documents

DVS website: http://disa.dtic.mil/disnvtc/become.htm

F.6 Sample Topology Diagrams

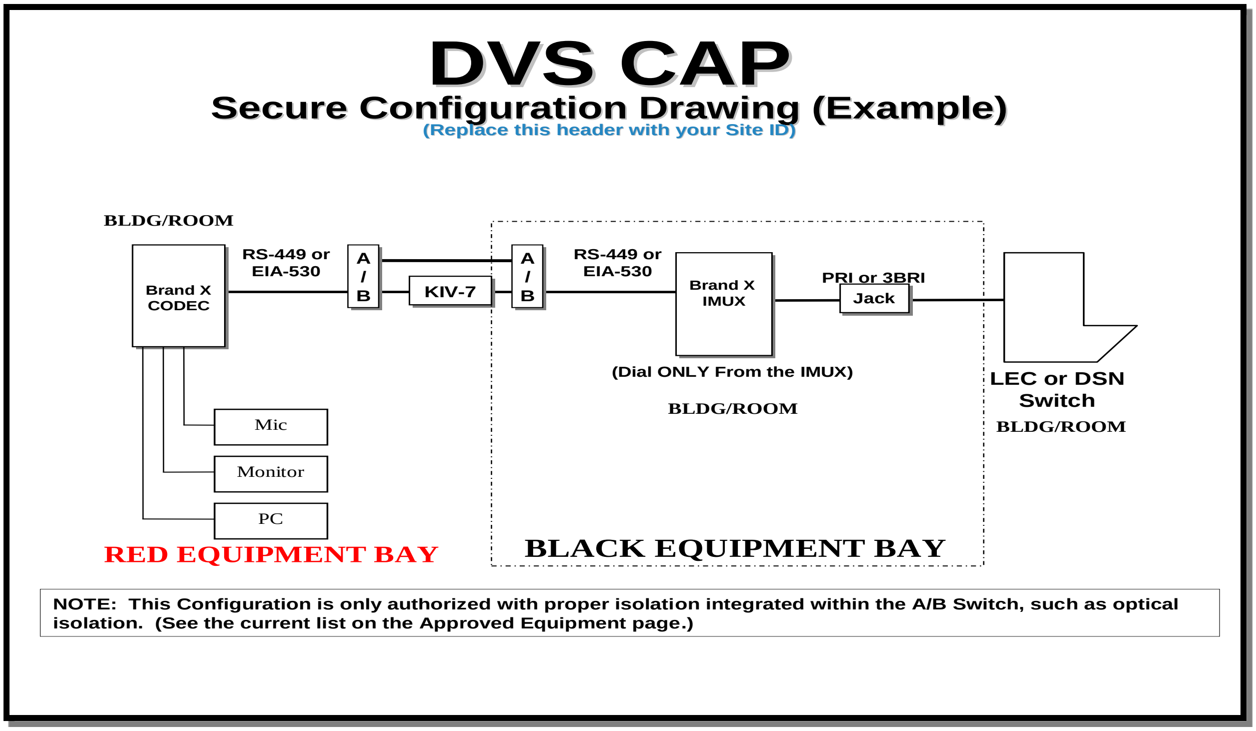
All configuration drawings must include the make and model of the Coder-Decoder (CODEC), Inverse Multiplexor (IMUX), Dial Isolator, and all switches. This information is required prior to processing your request for service or renewal of service.

The Video Teleconferencing Facility (VTF) connectivity diagram must include all associated devices including video equipment, Multipoint Control Units (MCUs), line interface units, hubs, IP connections, routers, firewalls, gateways, modems, encryption devices, backup devices, type of transport, bandwidth being utilized, your Site ID, and building/room locations of all equipment.



This Configuration is only authorized with proper isolation integrated within the A/B Switch, such as optical isolation. (See the current list on the Approved Equipment page.)

Figure 15 DVS Secure Configuration Drawing – Example 1



NOTE: This Configuration is only authorized with proper isolation integrated within the A/B Switch, such as optical isolation. (See the current list on the Approved Equipment page.)

Figure 16 DVS Secure Configuration Drawing – Example 2

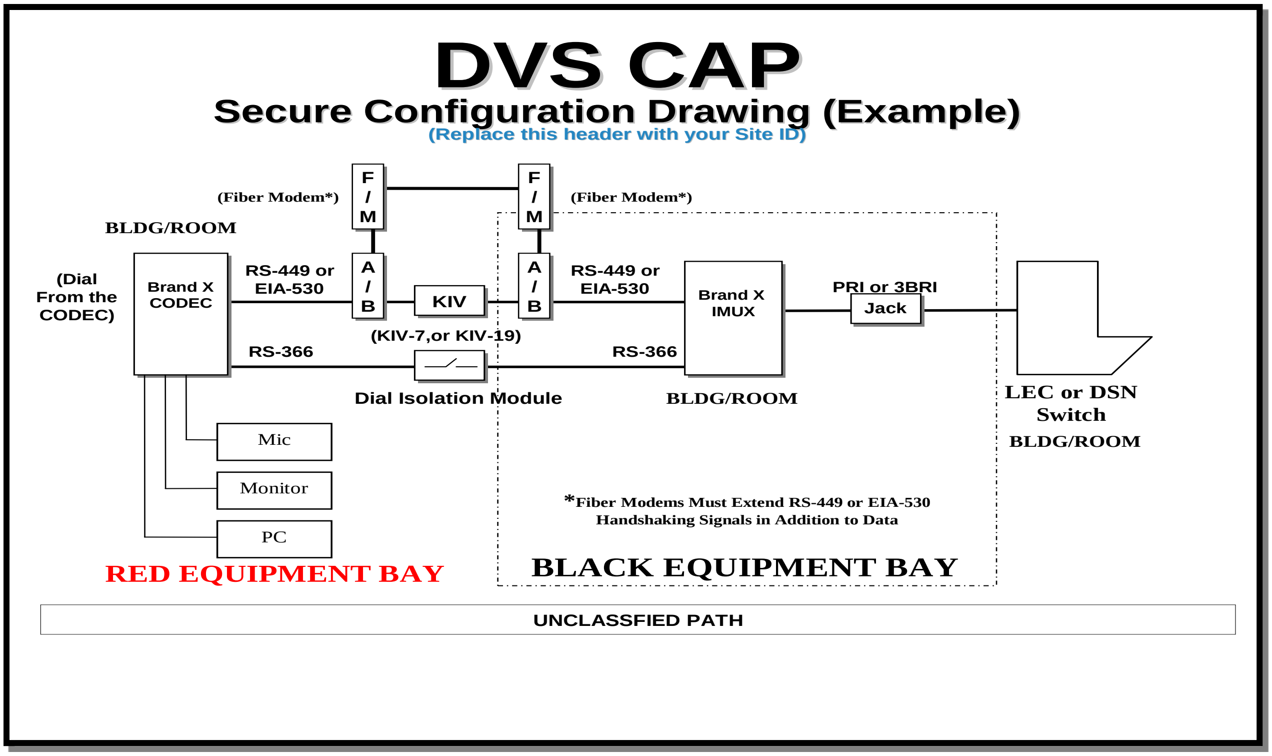


Figure 17 DVS CAP Secure Configuration Drawing – Example 3

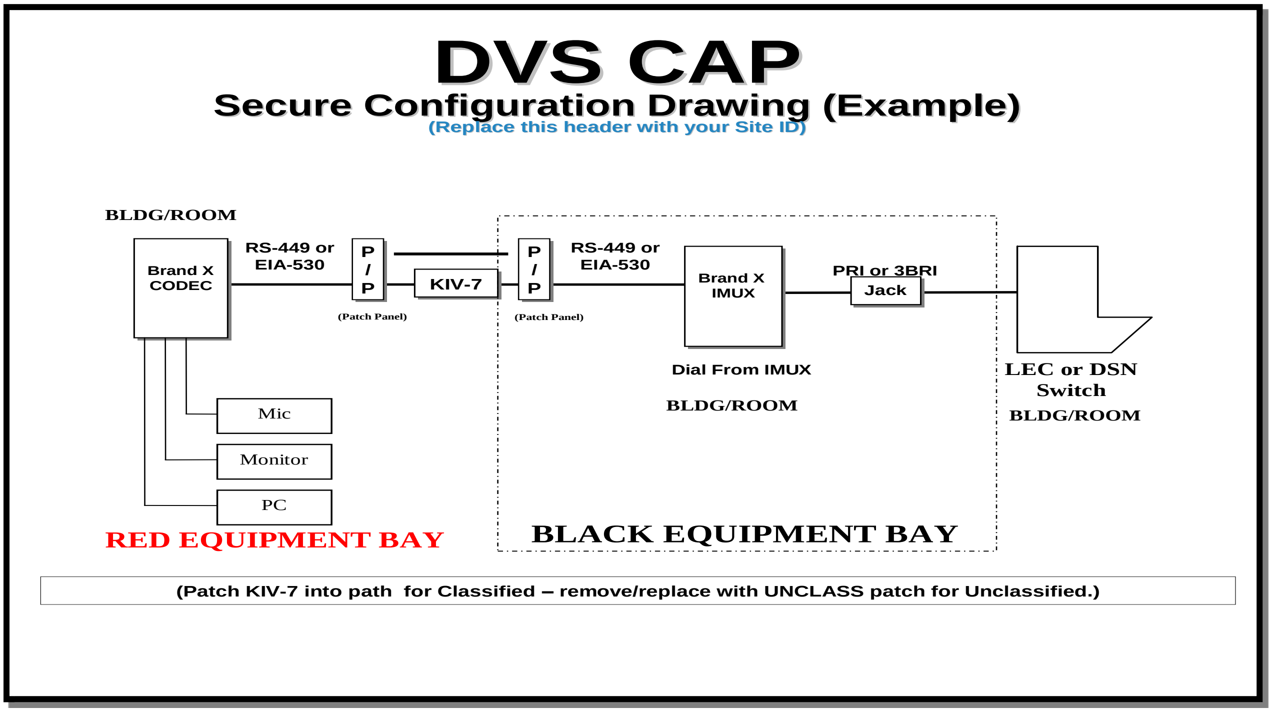
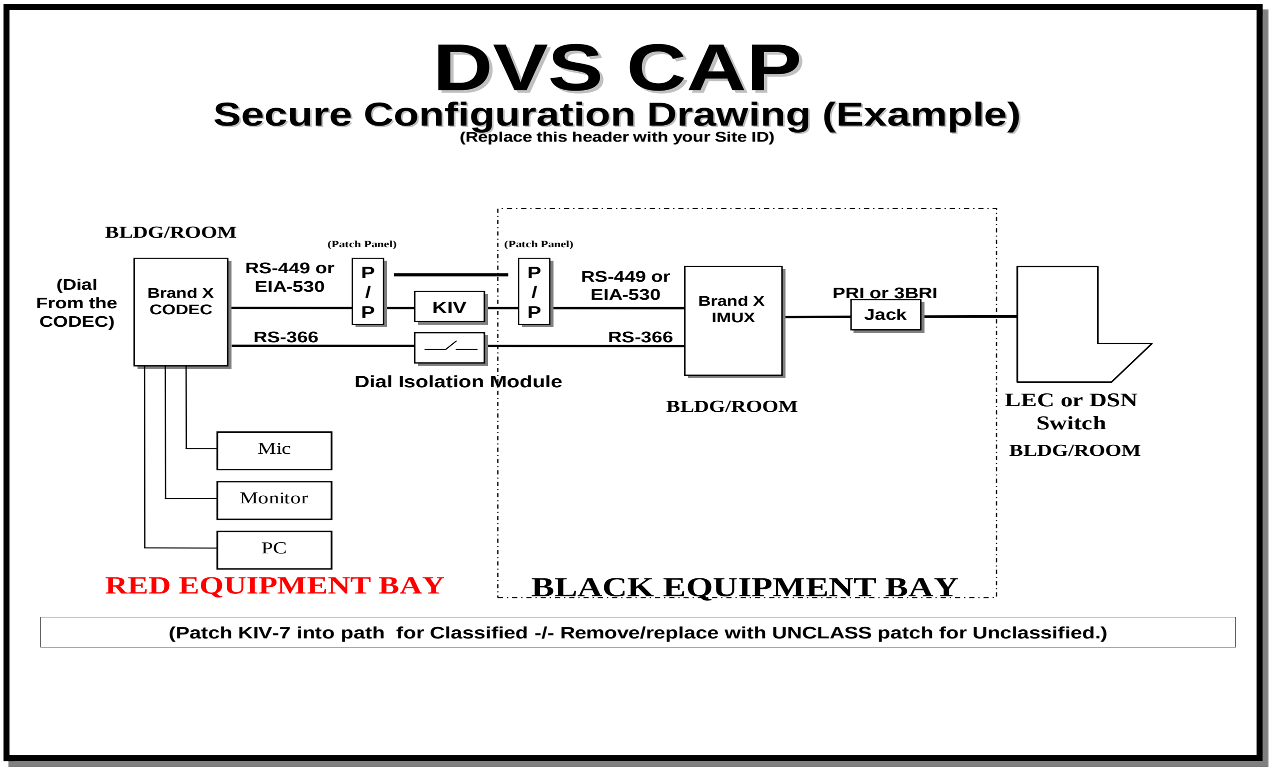


Figure 18 DVS CAP Secure Configuration Drawing – Example 4



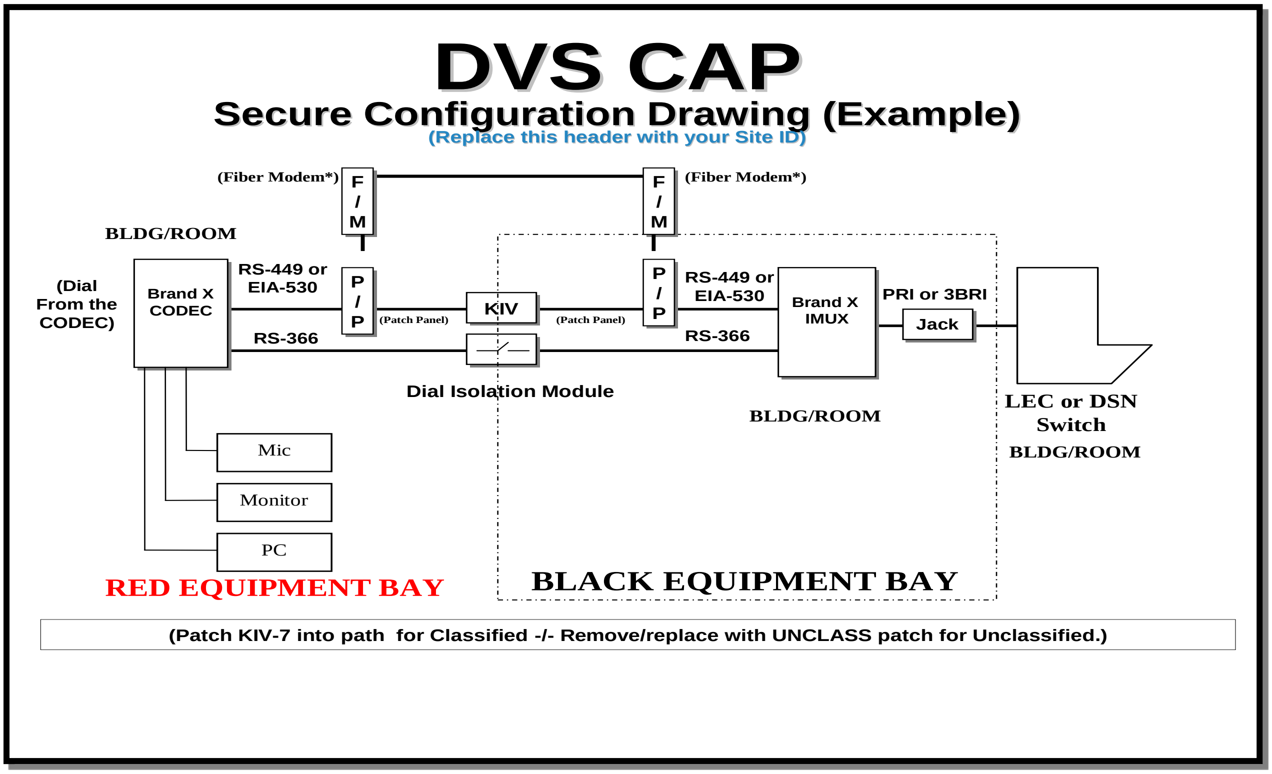
DVS CAP

Secure Configuration Drawing (Example)

(Replace this header with your Site ID)

(Patch KIV-7 into path for Classified -/- Remove/replace with UNCLASS patch for Unclassified.)

Figure 19 DVS CAP Secure Configuration Drawing – Example 5



DVS CAP

Secure Configuration Drawing (Example)

(Replace this header with your Site ID)

(Patch KIV-7 into path for Classified -/- Remove/replace with UNCLASS patch for Unclassified.)

Figure 20 DVS CAP Secure Configuration Drawing – Example 6

APPENDIX G

NIPRNET – UNCLASSIFIED

This appendix provides the necessary steps and information for a Non-classified Internet Protocol Router Network (NIPRNet) connection. It is intended to supplement the detailed information provided in Section 3 of this guide with NIPRNet-specific information. Any deviations or additional requirements are identified in this appendix.

G.1 NIPRNet Connection Process

Follow steps 1-12 in Section 3 of this guide.

G.2 Process Deviations and/or Additional Requirements

There are no additional requirements and/or process deviations.

G.3 NIPRNet Connection Process Checklist

This checklist provides the key activities that must be performed by the customer/sponsor during the NIPRNet connection approval process.

Item	DoD Customer		Non-DoD Customer	
	New	Existing	New	Existing
Obtain OSD approval for non-DoD connection			√	√[5]
Provision the connection	√		√	√[5]
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO/IATT)	√	√	√	√
Register the connection	√	√[6]	√	√[5]
Register in the SNAP database	√	√[6]	√	√[5]
Register in the PPSM database	√	√[6]	√	√[5]
Register with the SIPRNet Support Center (SSC)	√	√	√	√
Register in the DITPR database	√	√[6]	√	√[5]
Complete the CAP package	√	√	√	√
DIACAP Executive Package (or equivalent for non-DoD entities)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
DAA Appointment Letter	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
Proof of Contract			√	√
OASD(NII) Approval Letter			√	√
Submit the CAP package to the CAO	√	√	√	√
Receive NIPRNet ATC/IATC	√	√	√	√

Table 6 NIPRNet Connection Process Checklist

[5] This step is not required for existing non-DoD customer connections unless there has been a change in sponsor, mission requirement, contract, or location.

[6] This step is not required for existing connections that are already registered and all information is current.

G.4 Points of Contact

SIPRNet Support Center (SSC)	
Unclassified email	hostmaster@nic.mil
Phone (Commercial)	800-582-2567
Phone (DSN)	312-850-2713
Fax (Commercial)	614-692-3452
Fax (DSN)	312-850-3452
Website	www.ssc.smil.mil

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

Primary POCs

Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Phone (Commercial)	703-882-2086	703-882-2086, 301-225-2900/2901
Phone (DSN)	312-381-2086	312-381-2086, 312-761-2900/2901

NIPRNet Service Manager		BRAC Update Effective 16 May 2011
Phone (Commercial)	703-882-0158	301-225-2081
Phone (DSN)	312-381-0158	312-761-2081
Fax (Commercial)	703-882-2885	
Fax (DSN)	312-381-2885	

NIPRNet Customer Service		BRAC Update Effective 16 May 2011
Phone (Commercial)	703-882-0159	301-225-2083
Phone (DSN)	312-382-0159	312-761-2083
Fax (Commercial)	703-882-2885	
Fax (DSN)	312-381-2885	

U.S. Army

Army, Army National Guard, and Army Reserve organizations/offices with a requirement for NIPRNet service should contact US ARMY NETCOM, Ft. Huachuca, AZ.

NETCOM ESTA, ATD	
Phone (Commercial)	520-538-8029/8036
Phone (DSN)	312-879-8029/8036
Fax (Commercial)	520-538-0766

U.S. Air Force

For information on the AF NIPRNet provisioning process and AF DISN Subscription Service (DSS) locations, please contact:

AFCA DISN Command Lead	
Phone (Commercial)	618-229-6186/5732
Phone (DSN)	312-779-6186/5732

U.S. Navy/U.S. Marine Corps

USN and USMC organizations/offices with a requirement for NIPRNet service should contact:

NCMO Office of Record, Pensacola, FL	
Phone (Commercial)	850-452-7700
Phone (DSN)	312-992-7700

DISA Activities

Other DoD agencies should contact the DISA activity responsible for areas as indicated below:

Special user circuit requirements:

DISA National Capital Region (NCR)		BRAC Update Effective 16 May 2011
Unclassified email	provhqs@ncr.disa.mil	provhqs@ncr.disa.mil
Phone (Commercial)	703-882-0318/0322/0102/0330	
Phone (DSN)	312-381-0318	
Address	PO Box 4502 Arlington, VA 22204-4502	PO Box 549 Ft. Meade, MD 20755-0549

GIG Areas 1, 2, and inter-GIG:

DISA CONUS Provisioning Center	
Unclassified email	provtms@scott.disa.mil
Address	PO Box 25860 Scott AFB, IL 62225-5860

G.5 Additional Policy and Guidance Documents

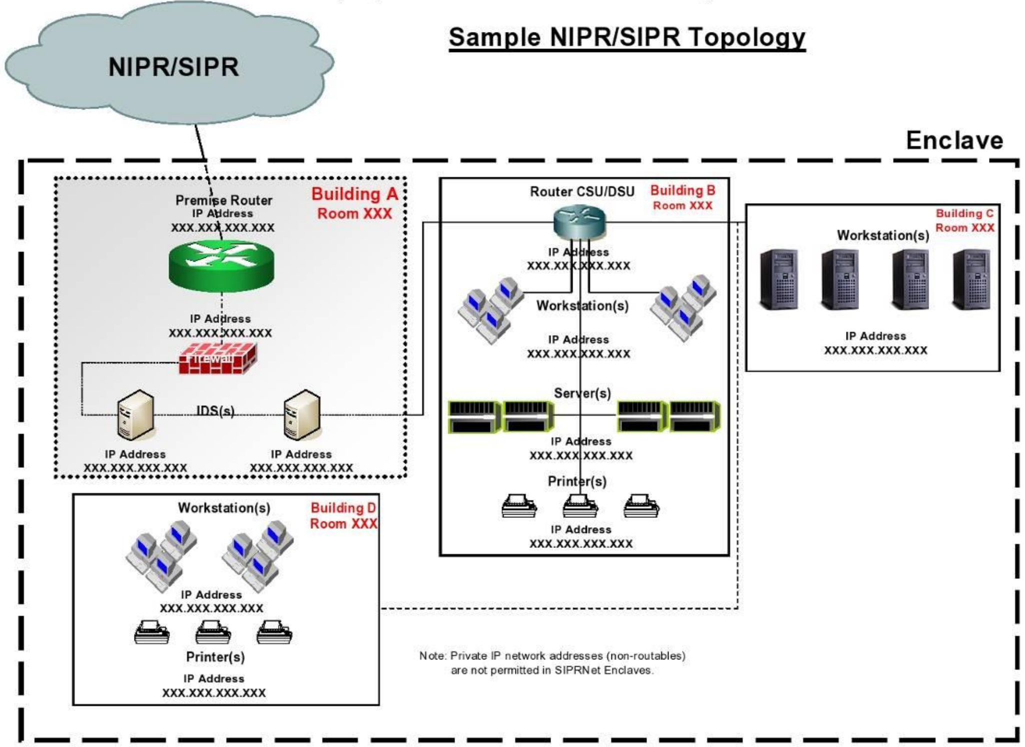
Formal completion and submission of ATC request is required. Go to the DSN ATC Request Submittal form at http://www.disa.mil/dsn/jic/atcsubmittal.html.

G.6 Sample Topology Diagram

All topologies must include:

- Topology date
- CCSD (preferably near premise router)
- IP addresses for all devices within the enclave, and the following devices must include additional information specific to them:
  - Firewalls: manufacturer, model, and software/firmware version
  - IDS: manufacturer, model, and software/firmware version
  - Enclave boundary premise route model and software version
  - Servers: server function (i.e., OWA, Web Server, etc.) and operating system (including most updated Service Pack installed on system)
  - Workstations: operating system (including most updated Service Pack installed on system)

All topologies must include IP addresses and ranges



Note: Private IP network addresses (non-routables) are not permitted in SIPRNet Enclaves.

Note: Please reference NIAP at http://www.niap-ccevs.org/cc-scheme/vpl/ for compliant device listing

Figure 21 NIPRNET/SIPRNET Topology Sample

***NOTE*:** *Please reference the NIAP-CCEVS at http://www.niap-ccevs.org for a listing of compliant devices.*

This page intentionally left blank.

APPENDIX H

OSD GIG WAIVER PROCESS - UNCLASSIFIED

If an alternative connection path (i.e., commercial Internet Service Provider (ISP)) is required for NIPRNet access (i.e., enclave/standalone), a waiver must be approved by the GIG Waiver Panel and signed by OASD(NII).

H.1 Baseline Commercial ISP Connection Approval Criteria

If DISA has determined that the CC/S/A/FA requirements cannot be fulfilled by DoD common user-systems, an exemption (i.e., GIG Waiver) may be requested by the CC/S/A/FA. These types of alternate connections require the OSD GIG Waiver Board to grant a waiver prior to operation.

DISA and DSAWG will review all CC/S/A/FA GIG waiver requests and provide a recommendation to the OSD GIG Waiver Panel prior to adjudication of the request. It is the responsibility of the CC/S/A/FA and the customer to present the GIG waiver request to the OSD GIG Waiver Panel. If the GIG waiver request is approved, the CC/S/A/FA shall utilize the appropriate DITCO contracting office to obtain the Internet service from a commercial ISP.

H.2 Process Deviations and/or Additional Requirements

<u>Documentation Requirements</u>
Develop a 20-minute (average time) PowerPoint slide briefing based on provided guidance and the waiver criteria. The briefing will cover the points below and be conducted at the Top Secret (TS) level or below. Soft copy of the briefing must be submitted electronically to DISA for review at least six weeks prior to the OSD GIG Waiver Panel meeting. The OSD GIG Secretariat shall be in receipt of all briefs, including DISA and DSAWG recommendations, at least two weeks in advance. This will be distributed to the voting members for review so that any questions can be provided to you for further clarification before the actual presentation. All CC/S/A/FA customers are required to coordinate the presentation with DISA. Briefs should be submitted to ucao-waivers@disa.mil.

- PowerPoint Brief
    - Cover slide will contain the Name of Component/Agency, Waiver Request Identification #, Date, CIO, and POC.
    - Mission of component/agency and of the network/computing function/satellite support/ISP.
    - What is it your organization does and how does the requirement support that mission?
    - Does the Organization’s Charter or DoD Directive drive a requirement?
    - What has DISA provided as a DISN solution and why does it not fulfill your requirement?
    - Other questions the panel/board will consider:
        - Is the requirement National Security System (NSS), command and control, mission essential?

    - What operational considerations merit deviation from the DoD DISN/GIG architecture?
    - Is this a requirement or a solution?
    - Is the time requirement valid?

- Architectural Congruence - Coordination with DISA is required to ensure DoD Global Information Grid (GIG) architecture compliance. Provide a communications diagram of current architecture and proposed architectures. At a minimum, the drawing must identify any Intrusion Detection Systems (IDSs), premise router, firewalls, any other security-related systems that are installed, and any connections to other systems/networks. If NIPRNet-to-Internet connection, identify the command communications service designators (CCSDs) of all connections to the DISN. Identifications to other connected systems should include the name of the organization that owns the system/enclave, the connection type (e.g., wireless, dedicated point-to-point), and the organization type (e.g., federal, DoD, contractor, etc.).

  - Other questions the panel/board will consider:

    - Basic architectural diagram.
    - Is this a defined technical requirement?
    - Is the request duplicative of other existing service?
    - Does this deviation from DoD architecture preserve interoperability?
    - Does this deviation from DoD architecture preserve positive control?
    - Does this deviation from DoD architecture enable network control?
    - Does this deviation from DoD architecture enable configuration management?
    - How much time will it take DISA to migrate the network to DISN?
    - Using current offerings, can DISA provide the services requested?
    - Will DISA expand current offerings to include the services requested?

- Business Case/Best Practices

  - How much will it cost? Include all costs. This must be coordinated with DISA.
  - Questions the panel/board will consider:
  - Is the request funded?
  - Is there a supporting business case?
  - If a service network solution is not possible, what is the business case for transport only solution?
  - Time requirement – Commercial Contract expires/Waiver expires.
  - Monthly Reoccurring or Annual Cost for the ISP connection.
  - What is the total cost to DoD?
  - Alternative Solutions – includes specifying why the CC/S/A/FA cannot use a Defense Information System Network (DISN) solution to perform the requirement being requested.
  - Cost Alternatives.
  - Plan for obtaining the commercial ISP connection through the appropriate DITCO contracting office.

- Accreditation - All DoD ISs require certification and accreditation through DIACAP (DoDI 8510.01 (ref g)). Waivers will not be processed further if the accreditation is not current. DAA approved Scorecard with expiration date should assert the DAA's acknowledgement of mission and connection requirements, and acceptance of the risk associated with deviation from standard architecture.

- Independent verification of physical and logical separation from the DoD network may be required.

H.3 OSD GIG Waiver Connection Approval Waiver Process Flow

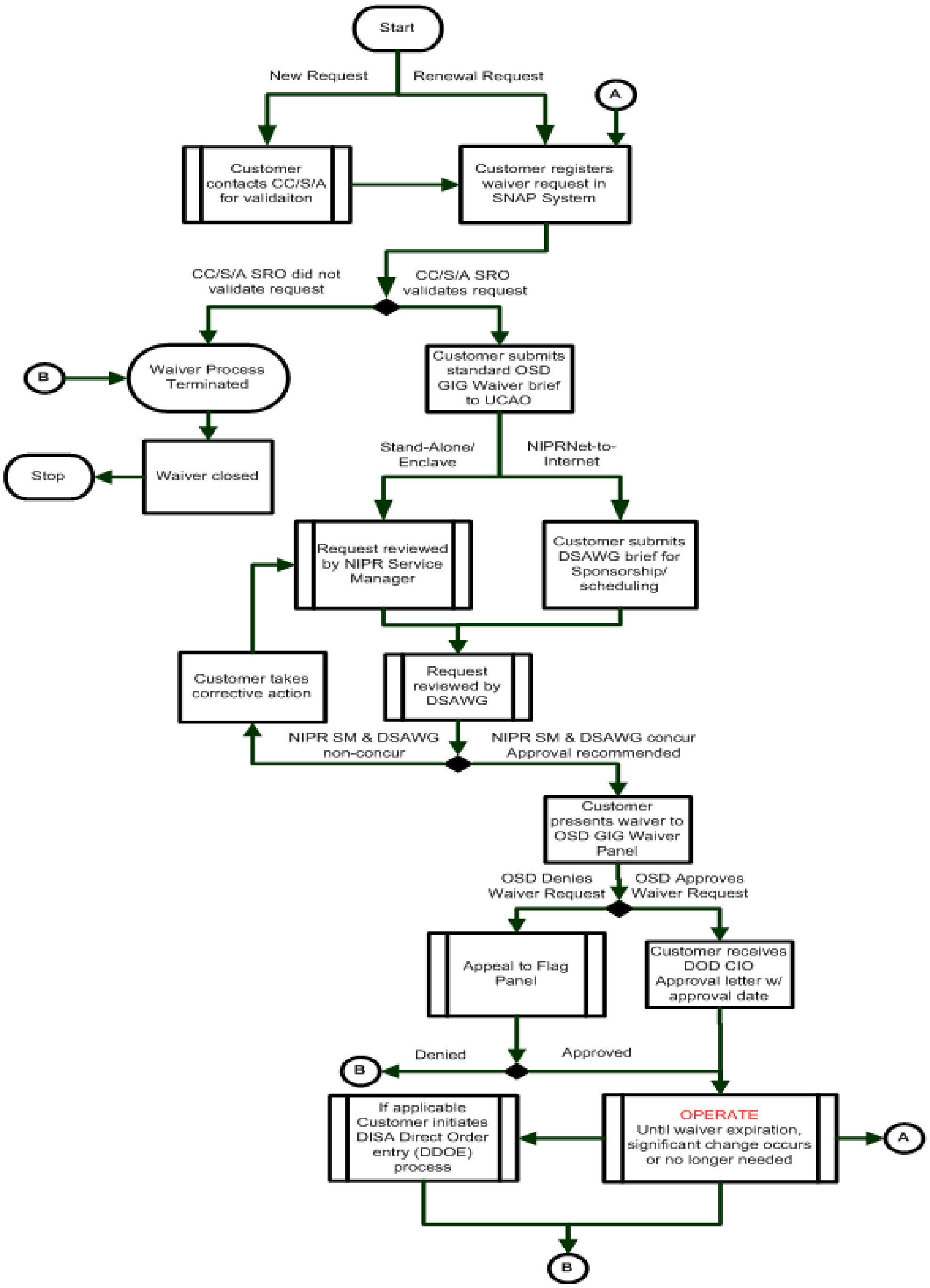

Start
New Request
Renewal Request
A
Customer contacts CC/S/A for validaiton
Customer registers waiver request in SNAP System
CC/S/A SRO did not validate request
CC/S/A SRO validates request
B
Waiver Process Terminated
Customer submits standard OSD GIG Waiver brief to UCAO
Stop
Waiver closed
Stand-Alone/ Enclave
NIPRNet-to-Internet
Request reviewed by NIPR Service Manager
Customer submits DSAWG brief for Sponsorship/ scheduling
Customer takes corrective action
Request reviewed by DSAWG
NIPR SM & DSAWG non-concur
NIPR SM & DSAWG concur Approval recommended
Customer presents waiver to OSD GIG Waiver Panel
OSD Denies Waiver Request
OSD Approves Waiver Request
Appeal to Flag Panel
Customer receives DOD CIO Approval letter w/ approval date
Denied
Approved
B
If applicable Customer initiates DISA Direct Order entry (DDOE) process
OPERATE
Until waiver expiration, significant change occurs or no longer needed
A
B

Figure 22 OSD GIG Waiver Process

H.4 Points of Contact

Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Unclassified email	ucao-waivers@disa.mil	ucao-waivers@disa.mil
Phone (Commercial)	703-882-0138	703-882-0138, 301-225-2900/2901

H.5 Additional Policy and Guidance Documents

CJCSI 6211.02C	*Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 (ref a)
DoDD 8500.01E	*Information Assurance (IA)*, 24 October 2002 (ref c)
DoDI 8500.2	*Information Assurance (IA) Implementation*, 6 February 2003 (ref f)
DoDI 8100.4	*DoD Unified Capabilities*, 9 December 2010 (ref o)

APPENDIX I

REAL TIME SERVICES – CLASSIFIED AND UNCLASSIFIED

(THIS APPENDIX IS STILL UNDER DEVELOPMENT.)

This page intentionally left blank.

APPENDIX J

SIPRNET – CLASSIFIED

This appendix provides the necessary steps and information for a Secret Internet Protocol Router Network (SIPRNet) connection. It is intended to supplement the detailed information provided in Section 3 of this guide with SIPRNet-specific information. Any deviations from those or additional requirements are identified in this appendix.

J.1 SIPRNet Connection Process

Follow steps 1-12 in Section 3 of this guide.

J.2 Process Deviations and/or Additional Requirements

Step 8 DoD Contractor connections to the SIPRNet must go through DSS for accreditation of their facilities and information systems. For questions regarding DSS accreditation, contact the DSS SIPRNet Program Management Office at occ.cust.serv@dss.mil by phone at 888-282-7682, Option 2.

Step 10 All DoD and non-DoD customers/sponsors must complete the SIPRNet Connection Questionnaire (SCQ) and submit it with the CAP package. The DAA is responsible for the content of the SCQ but may delegate the signatory responsibility to a lower level. The SCQ is available on the CAO web page at www.disa.mil/connect/library.

- All 'Yes' responses must be explained, with the exception of questions 14, 15, and 16
- All POC information must be completed for the questionnaire to be accepted by the CAO

Step 11 The CAO review of the SIPRNet CAP package for new connections includes an on-line remote compliance assessment. This is a vulnerability scan of the IS requesting SIPRNet connection, performed by the CAO, to identify possible vulnerabilities that exist within the IS. The results are used during the connection approval decision-making process.

J.3 SIPRNet Connection Process Checklist

This checklist provides the key activities that must be performed by the customer/sponsor during the SIPRNet connection approval process.

Item	DoD Customer		Non-DoD Customer	
	New	Existing	New	Existing
Obtain OSD approval for non-DoD connection			√	√[7]
Provision the connection	√		√	√[7]
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO)	√	√	√	√
Register the connection	√	√[8]	√	√[7]
Register in the GIAP/SGS database	√	√[8]	√	√[7]
Register in the PPSM database	√	√[8]	√	√[7]
Register in the SIPRNet IT Registry database	√	√[8]	√	√[7]
Register with the SIPRNet Support Center (SSC)	√	√[8]	√	√[7]
Complete the CAP package	√	√	√	√
DIACAP Executive Package (or equivalent for non-DoD entities)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
DAA Appointment Letter	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
SIPRNet Connection Questionnaire (SCQ)	√	√	√	√
Proof of Contract			√	√
OASD(NII) Approval Letter			√	√[7]
Submit the CAP package to the CAO	√	√	√	√
Receive remote compliance scan	√		√	
Receive SIPRNet ATC/IATC	√	√	√	√

Table 7 SIPRNet Connection Process Checklist

[7] This step is not required for existing non-DoD Customer connections unless there has been a change in sponsor, mission requirement, contract, or location.

[8] This step is not required for existing connections that are already registered and all information is current.

J.4 Points of Contact

SIPRNet Support Center (SSC)	
Unclassified email	hostmaster@nic.mil
Phone (Commercial)	800-582-2567
Phone (DSN)	312-850-2713
Fax (Commercial)	614-692-3452
Fax (DSN)	312-850-3452
Website	www.ssc.smil.mil

SIPRNet Service Manager	
Phone (Commercial)	301-225-2484

SIPRNet Support Center (SSC)	
Phone (Commercial)	800-582-2567/703-821-6260

Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Unclassified email	CCAO@disa.mil	CCAO@disa.mil
Classified email	CCAO@disa.smil.mil	CCAO@disa.smil.mil
Phone (Commercial)	703-882-1455	703-882-1455, 301-225-2900/2901
Phone (DSN)	312-381-1455	312-381-1455, 312-761-2900/2901
Fax (Commercial)	703-882-2813	703-882-2813
Fax (DSN)	312-381-2813	312-381-2813

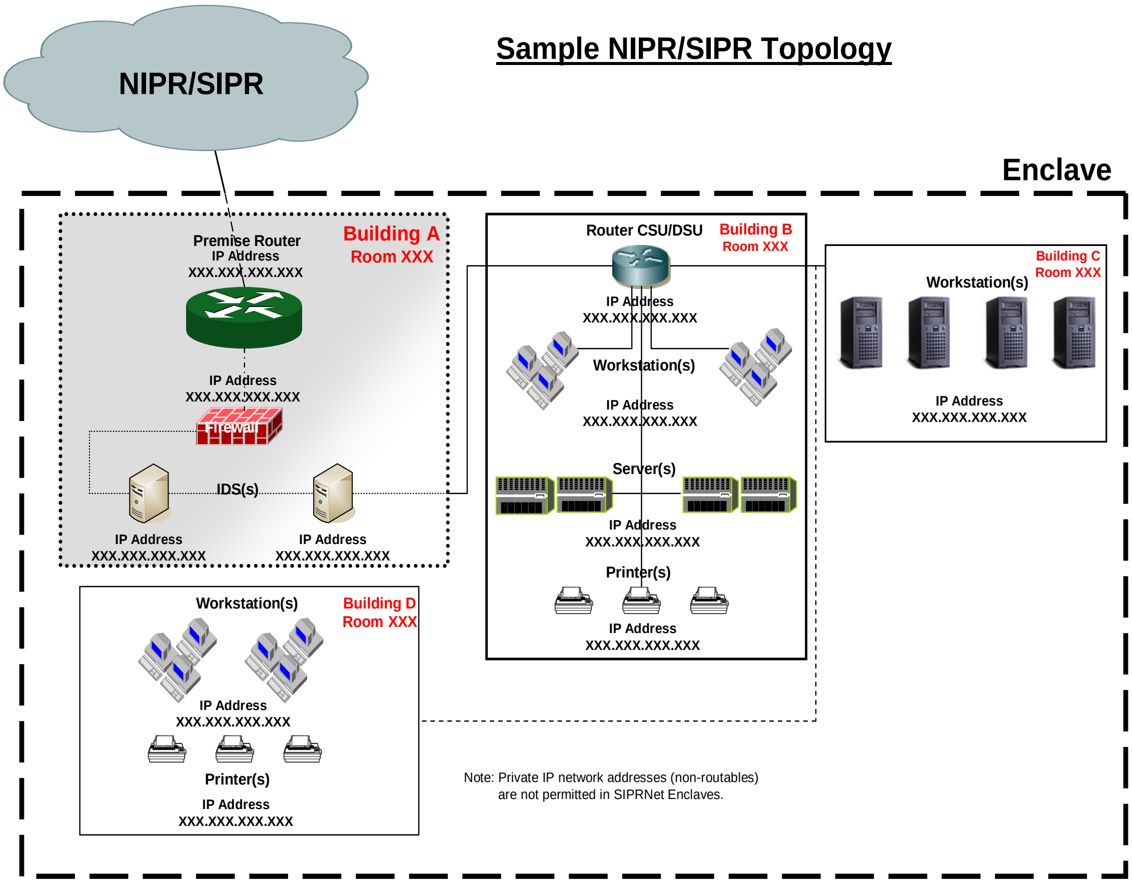
J.5 Additional Policy and Guidance Documents

Cross Domain Solutions (CDS) are a special case of the SIPRNet connection process. Please refer to the CDS Process (Appendix K) for more information.

J.6 Sample NIPRNET/SIPRNET Topology

All topologies must include:

- Topology date
- CCSD (preferably near premise router)
- Internetworking Operating System (IOS) version
- IP addresses for all devices within the enclave, and the following devices must include additional information specific to them:
    - Firewalls: manufacturer, model, and software/firmware version
    - IDS: manufacturer, model, and software/firmware version
    - Servers: server function (i.e., OWA, Web Server, etc.) and operating system (including most updated Service Pack installed on system)
    - Workstations: operating system (including most updated Service Pack installed on system)



Note: Please reference NIAP at http://www.niap-ccevs.org/cc-scheme/vpl/ for compliant device listing

Figure 23 NIPRNET/SIPRNET Topology Sample 2

APPENDIX K

CDS – CLASSIFIED AND UNCLASSIFIED

Cross Domain Solutions (CDS) require an additional approval process and authorization, separate from the review and approval for the ATC for the CCSD. This appendix provides the steps necessary to obtain a Cross Domain Solution Authorization (CDSA).

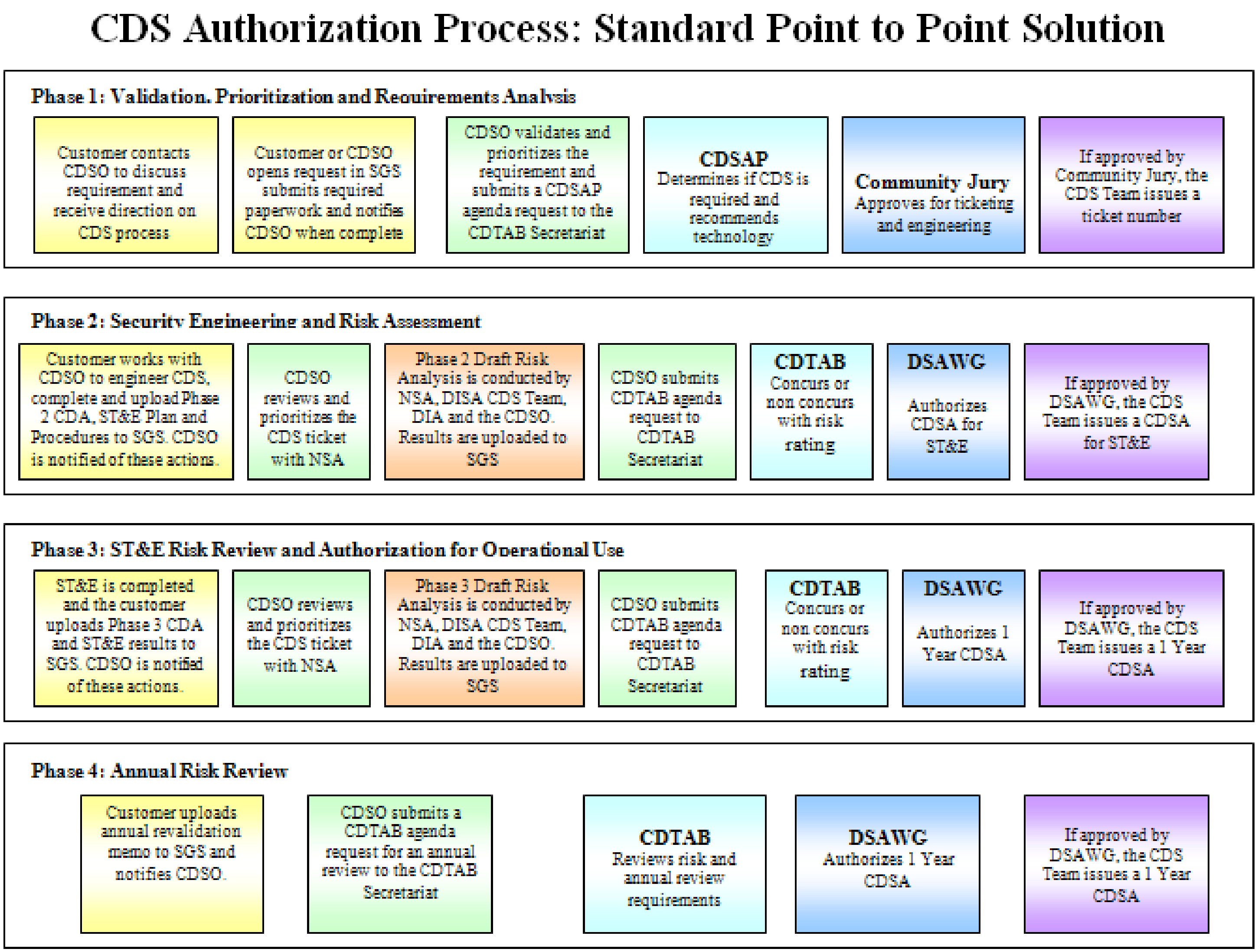
NOTE: *This process covers CDS devices connecting to networks classified Top Secret and below. CDS devices connecting to networks classified Top Secret – SCI and above follow a different approval process outlined by the Unified Cross Domain Management Office and DIA.*

K.1 Mandatory CDS Requirements for Connection to the SIPRNet

Customers are required to follow the guidelines below to obtain connection approval for their CDS devices. A CDSA will not be granted unless all required documentation and approvals have been completed. There are two main CDS processes, those for Standard Point-to-Point Solutions (covered in K.2) and DISA's Cross Domain Enterprise Services (CDES) (covered in K.3).

K.2 CDS Authorization Process: Standard Point-to-Point Solution

The CDS Authorization process for Standard Point-to-Point Solutions is comprised of four phases: Phase 1 - Validation, Prioritization, and Requirements Analysis; Phase 2 - Solution Development and Risk Assessment; Phase 3 - Security Engineering and Risk Assessment; and Phase 4 - Annual Risk Review. The following diagram presents a graphical depiction of the CDS process.



CDS Authorization Process: Standard Point to Point Solution

Phase 1: Validation, Prioritization and Requirements Analysis

Customer contacts CDSO to discuss requirement and receive direction on CDS process

Customer or CDSO opens request in SGS submits required paperwork and notifies CDSO when complete

CDSO validates and prioritizes the requirement and submits a CDSAP agenda request to the CDTAB Secretariat

CDSAP Determines if CDS is required and recommends technology

Community Jury Approves for ticketing and engineering

If approved by Community Jury, the CDS Team issues a ticket number

Phase 2: Security Engineering and Risk Assessment

Customer works with CDSO to engineer CDS, complete and upload Phase 2 CDA, ST&E Plan and Procedures to SGS. CDSO is notified of these actions.

CDSO reviews and prioritizes the CDS ticket with NSA

Phase 2 Draft Risk Analysis is conducted by NSA, DISA CDS Team, DIA and the CDSO. Results are uploaded to SGS

CDSO submits CDTAB agenda request to CDTAB Secretariat

CDTAB Concurs or non concurs with risk rating

DSAWG Authorizes CDSA for ST&E

If approved by DSAWG, the CDS Team issues a CDSA for ST&E

Phase 3: ST&E Risk Review and Authorization for Operational Use

ST&E is completed and the customer uploads Phase 3 CDA and ST&E results to SGS. CDSO is notified of these actions.

CDSO reviews and prioritizes the CDS ticket with NSA

Phase 3 Draft Risk Analysis is conducted by NSA, DISA CDS Team, DIA and the CDSO. Results are uploaded to SGS

CDSO submits CDTAB agenda request to CDTAB Secretariat

CDTAB Concurs or non concurs with risk rating

DSAWG Authorizes 1 Year CDSA

If approved by DSAWG, the CDS Team issues a 1 Year CDSA

Phase 4: Annual Risk Review

Customer uploads annual revalidation memo to SGS and notifies CDSO.

CDSO submits a CDTAB agenda request for an annual review to the CDTAB Secretariat

CDTAB Reviews risk and annual review requirements

DSAWG Authorizes 1 Year CDSA

If approved by DSAWG, the CDS Team issues a 1 Year CDSA

Figure 24 CDS Connection Process

K.2.1 Phase 1 CDS Authorization Process: Point-to-Point Solution

Validation, Prioritization and Requirements Analysis

Phase 1 of the CDS process consists of six specific actions. Any exceptions to the CDS process must be coordinated with your CC/S/A representatives and Cross Domain Technical Advisory Board (CDTAB) chair. The first three actions must be completed in 45 days.

1. The CDS customer must coordinate with the CC/S/A Cross Domain Solutions Organization (CDSO) representatives to determine and document the information transfer and mission requirements. These requirements must be documented on the Cross Domain Appendix (CDA).

   NOTE: *All COCOMs must utilize the CDSO represented by their supporting agency as referenced in* DoDD 5100.3, *Support of the Headquarters of Combatant and Subordinate Joint Commands,* 15 November 1999 (ref t). *It is the CDSO's CDTAB Representative's responsibility to complete the Transfer Processing Threat Report and to submit a request for an agenda to be presented to the Cross Domain Solutions Assessment Panel (CDSAP) or CDTAB.*

2. Customer or CDSO obtains access to the SGS (https://giap.disa.smil.mil) through the CAO, opens a new CDS request filling out all required database fields, uploads a Phase 1 CDA, a validation memo signed by their respective DAA, and notifies their CDSO of completion of these requirements.
3. The customer's respective CDSO validates and prioritizes the Request and submits a CDSAP agenda request to the CDTAB Secretariat. ***NOTE:*** *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*
4. The request (in the form of a request number) is brought before the CDSAP to determine if a CDS is required to meet the customer's requirement and if the proposed solution versus an alternative solution is recommended. The CDSAP also determines if DISA's CDES could be utilized to meet the customer's requirement. This determination is then presented to the Community Jury in Step 5.
5. The CDS Request and CDSAP comments are brought before the Community Jury (a function of the DSAWG) to obtain approval for ticketing and engineering.
6. If approved by the Community Jury and the CDS is going to be implemented as a point-to-point solution, the CDS team will assign a CDS ticket number and the CDS is transitioned into Phase 2. If approved by the Community Jury and DISA CDES is going to meet the requirement, the request number will be closed and the requirement will be met under a CDES ticket number (see K.3).

K.2.2 Phase 2 CDS Authorization Process: Point-to-Point Solution

Security Engineering and Risk Assessment

1. The customer works with their respective CDSO to engineer the CDS, and to complete, and upload the following to the SGS: 1) Phase 2 CDA, 2) a Security, Test, and Evaluation (ST&E) Plan; and 3) ST&E Procedures. The customer notifies the CDSO when all requirements have been met. ***NOTE:*** *The customer should contact their respective CDSO if they have questions or need assistance with completing the required content in the referenced documents.*
2. The respective CDSO reviews and prioritizes the CDS ticket with NSA who completes the bulk of the draft risk analysis report.
3. Draft risk analysis results are completed by NSA, the respective CDSO, the CDS Team, and DIA following the Risk Decision Authority Criteria (RDAC) criteria. These results must be uploaded to SGS.
4. The respective CDSO submits a CDTAB agenda request to the CDTAB Secretariat. ***NOTE:*** *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*
5. At the CDTAB, the voting members will review the information provided from the customer's CDA and the compiled risk rating then provide a vote of concur or non-concur with the risk rating.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a CDSA for ST&E.

   If approved and all other enclave documentation has met standard requirements, the CDS team will issue a CDSA for ST&E and the CDS ticket transitions into Phase 3. ***NOTE:*** *The CDS team will not issue a CDSA without the customer's ATO, SCQ, and topology referencing the specific ticket number of the CDS.*

K.2.3 Phase 3 CDS Authorization Process: Point-to-Point Solution

ST&E Risk Review and Authorization for Operational Use

1. Upon completion of the ST&E, the customer must upload the ST&E results and updated Phase 3 CDA to the SGS. The customer notifies the CDSO of these actions.
2. The respective CDSO reviews and prioritizes the CDS ticket with NSA who completes the bulk of the draft risk analysis report.
3. Draft Risk Analysis results are completed by NSA, the respective CDSO, the CDS Team, and DIA following the RDAC criteria. These results must be uploaded to SGS.
4. The respective CDSO submits a CDTAB agenda request to the CDTAB Secretariat. ***NOTE:*** *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*

5. At the CDTAB, the voting members will review the information provided from the customer's CDA and the compiled risk rating and provide a vote of concur or non-concur with the risk rating and comments.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a one-year CDSA.
7. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a one-year CDSA. The CDS ticket transitions into Phase 4. ***NOTE:*** *The CDS Team will not issue a CDSA without the customer's ATO, SCQ, and topology referencing the specific ticket number of the CDS.*

   NOTE: *The CDS device is marked operational in SGS upon the initial issuance of a CDSA by the* CDS Team *following a DSAWG approval. It remains operational until the CDTAB Secretariat receives evidence from the DAA through the customer's respective CDSO that the device is non-operational.*

K.2.4 Phase 4 CDS Authorization Process: Point-to-Point Solution

Annual Risk Review

CDS's will receive no more than a 1-year CDSA from the DSAWG. In order to receive approval for following years, the following requirements must be met.

1. Complete a satisfactory scan of the enclave by the CAO (or a POA&M if unsatisfactory); a satisfactory Command Cyber Readiness Inspection (CCRI) review of the enclave, submit a revalidation memo from the DAA stating that the CDS is still required and the CDS configuration has not changed, and notification provided to the CDSO of completion of the actions.

   NOTE*: Para 14 of Enclosure B to CJCSI 6211.02c (ref a) requires the DAA to revalidate all CDS devices in enclaves containing CDS devices annually. The DAA revalidate operational and functional requirements, verify the configuration described in the CDS documentation is correct, ensure and validate annual testing of CDS controls, operational requirements, configuration, and notify the respective CDSO that this review has been conducted. This notification should be in the form of an annual revalidation letter and should be uploaded to SGS under the respective CDS ticket number.*

2. The respective CDSO submits a CDTAB agenda request to the CDTAB Secretariat. ***NOTE:*** *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*
3. At the CDTAB, the voting members will review the CDS Annual Review requirements, information provided extracted from the customer's CDA and the previous risk rating, and provide a vote of concur or non-concur with the risk rating and comments.
4. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a 1-year CDSA.
5. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a 1-year CDSA. The CDS Ticket will remain in

Phase IV. ***NOTE:*** *The* CDS Team *will not issue a CDSA without the customer's ATO, SCQ, and topology referencing the specific ticket number of the CDS.*

***NOTE**: Desired changes to the configuration of the CDS including patches and upgrades must be coordinated with the customer's respective CDSO and entered into the SGS as Phase I requests. These requests must follow the normal CDS review process and be approved by the DSAWG prior to implementation.*

K.3 CDS Authorization Process: Cross Domain Enterprise Services

The CDS Authorization process for Cross Domain Enterprise Services (CDES) is comprised of four phases: Phase 1 - Validation, Prioritization, and Requirements Analysis; Phase 2 - Solution Development and Risk Assessment; Phase 3 - Security Engineering and Risk Assessment; and Phase 4 - Annual Risk Review.

The process is slightly different for a customer request being added to a new CDES solution vice an existing CDES solution. If the request is going to be added to an existing CDES solution, they will enter the CDES process at Phase 2. If the request is going to be met by a new CDES solution, they will enter the CDES process at Phase 1 and essentially will be going through Phase 1 twice, since they already went through the same Phase 1 as a point-to-point solution.

K.3.1 Phase 1 CDS Authorization Process: CDES

Validation, Prioritization, and Requirements Analysis

Phase 1 of the CDS process consists of six specific actions. Any exceptions to the CDS process must be coordinated with your CC/S/A representatives and Cross Domain Technical Advisory Board (CDTAB) chair. The first three actions must be completed in 45 days. In order for CDES to go forward with a request to build a new CDES solution, they must come forward with an already approved customer request that is awaiting implementation in the Enterprise. This is because DSAWG will not approve building a new solution if there is not a customer requirement for that solution.

1. CDES must coordinate with the DISA Cross Domain Solutions Organization (CDSO) representatives to determine and document the information transfer and mission requirements based on a previously approved customer request. These requirements must be documented on the Cross Domain Appendix (CDA).
2. CDES opens a new CDS request in the SGS filling out all required database fields, uploads a Phase 1 Cross Domain Appendix (CDA), and notifies their CDSO of completion of these requirements.
3. The customer's respective CDSO validates and prioritizes the Request and submits a CDSAP agenda request to the CDTAB Secretariat. ***NOTE:*** *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*
4. The request (in the form of a Request Number) is brought before the CDSAP to determine if a CDS is required to meet the customer's requirement and if the proposed solution versus an

alternative solution is recommended. This determination is then presented to the Community Jury in Step 5.

5. The CDES Request and CDSAP comments are brought before the Community Jury (a function of the DSAWG) to obtain approval for ticketing and engineering.
6. If approved by the Community Jury the CDS Team will assign a CDS Ticket Number and the CDES Request is transitioned into Phase II.

K.3.2 Phase 2 CDS Authorization Process: CDES

Security Engineering and Risk Assessment

NOTE: *If the customer request has already been approved by the Community Jury and is going to be added to preexisting CDES solution, the request will enter the CDES process at this phase (see 1.b).*

1. New or Existing CDES:
   a. **New CDES:** CDES works with DISA CDSO to engineer the CDS, complete, and upload the following to the SGS: 1) Phase II CDA, 2) an ST&E Plan; and 3) ST&E Procedures. CDES notifies the CDSO when all requirements have been met.

      NOTE: *CDES should contact DISA CDSO if they have questions or need assistance with completing the required content in the referenced documents.*

   b. **Existing CDES:** CDES notifies the CDSO and the CDS Team of intention to implement a Community Jury approved customer request (or multiple requests) under a new implementation of an existing CDS Ticket and requests CDS Team to issue a ticket number for that purpose. CDES works with DISA CDSO to engineer the CDS, complete, and upload the following to the SGS: 1) Phase II CDA, 2) a ST&E Plan; and 3) ST&E Procedures. CDES notifies the CDSO when all requirements have been met.
2. DISA CDSO reviews and prioritizes the CDS ticket with NSA who completes the bulk of the draft risk analysis report.
3. Draft Risk Analysis results are completed by NSA, the respective CDSO, the CDS Team, and DIA following the Risk Decision Authority Criteria (RDAC) criteria. These results must be uploaded to SGS.
4. DISA CDSO submits a CDTAB agenda request to the CDTAB Secretariat.

   NOTE: *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer or CDES.*
5. At the CDTAB the voting members will review the information provided from the customer's CDA and the compiled risk rating and provide a vote of concur or non-concur with the risk rating.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a CDSA for ST&E.
7. If approved and all other enclave documentation has met standard requirements, the CDS Team will issue a CDSA for ST&E and the CDS ticket transitions into Phase III. ***NOTE:***

The CDS Team *will not issue a CDSA without the customer's ATO, SCQ, and Topology referencing the specific ticket number of the CDS.*

K.3.3 Phase 3 CDS Authorization Process: CDES

ST&E Risk Review and Authorization for Operational Use

1. Upon completion of the ST&E CDES must upload the ST&E results and updated Phase III CDA to the SGS. CDES notifies the DISA CDSO of these actions.
2. DISA CDSO reviews and prioritizes the CDS ticket with NSA who completes the bulk of the draft risk analysis report.
3. Draft Risk Analysis results are completed by NSA, the DISA CDSO, the CDS Team, and DIA following the RDAC criteria. These results must be uploaded to SGS.
4. DISA CDSO submits a CDTAB agenda request to the CDTAB Secretariat.

   NOTE: *All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*
5. At the CDTAB, the voting members will review the information provided from the CDES CDA and the compiled risk rating and provide a vote of concur or non-concur with the risk rating and comments.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a 1-year CDSA.
7. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a 1-year CDSA. The CDS Ticket transitions into Phase IV. ***NOTE:*** *The* CDS Team *will not issue a CDSA without the customer's ATO, SCQ, and topology referencing the specific ticket number of the CDS.*

   NOTE: *The CDS device is marked operational in SGS upon the initial issuance of a CDSA by the CDS Team following a DSAWG approval. It remains operational until the CDTAB Secretariat receives evidence from the DAA through the customer's respective CDSO that the device is non-operational.*

K.3.4 Phase 4 CDS Authorization Process: CDES

Annual Risk Review for CDES Solutions

CDS's will receive no more than a one-year CDSA from the DSAWG. In order to receive approval for following years, the following requirements must be met.

NOTE: *This process is currently under review for CDES and will be revised in the next version of the CPG Appendix K.*

1. Complete a satisfactory scan of the enclave by the CAO (or a POA&M if unsatisfactory); a satisfactory Command Cyber Readiness Inspection (CCRI) review of the enclave, submit a revalidation memo from the DAA stating that the CDS is still required and the CDS configuration has not changed, and notification provided to the CDSO of completion of the actions.

***NOTE**: Para 14.8 of Enclosure B to CJCSI 6211.02c requires the DAA to revalidate all CDS devices in enclaves containing CDS devices annually. The DAA revalidate operational and functional requirements, verify the configuration described in the CDS documentation is correct, ensure and validate annual testing of CDS controls, operational requirements, configuration, and notify the DISA CAO office that this review has been conducted. This notification should be in the form of an annual revalidation letter and should be uploaded to SGS under the respective CDS ticket number.*

2. DISA CDSO submits a CDTAB agenda request to the CDTAB Secretariat.

   ***NOTE:** All agenda requests must be submitted by the respective CDSO to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the customer.*

3. At the CDTAB, the voting members will review the CDS Annual Review requirements, information provided extracted from the customer's CDA and the previous risk rating, and provide a vote of concur or non-concur with the risk rating and comments.
4. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a 1-year CDSA.
5. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a 1-year CDSA. The CDS Ticket will remain in Phase IV. ***NOTE:** The* CDS Team *will not issue a CDSA without the customer's ATO, SCQ, and topology referencing the specific ticket number of the CDS.*

   ***NOTE:** Desired changes to the configuration of the CDS including patches and upgrades must be coordinated with the customer's respective CDSO and entered into the SGS as Phase I requests. These requests must follow the normal CDS review process and be approved by the DSAWG prior to implementation.*

K.4 Frequently Asked Questions

K.4.1 Frequently Asked Questions

1. Q. Do I need to create a request for every CDS device/distribution console I intend to meet a specific requirement? What if it is a hot or cold spare or being used for load balancing?

   A. A separate request/ticket is required for each CDS device/distribution console if the device is used as a hot spare or load balancing. A separate request is not needed for a cold spare but the cold spare must go through ST&E with the primary and evidence of the ST&E results must be uploaded under the SGS. In the event the cold spare is utilized, the CDSO and CDS Team must be notified and a new request must be opened.

2. Q. What is the significance of the three partitions of a CDS ticket number?

A. Once a Request (ex: R0001111) is approved at Community Jury, it is assigned a ticket number that is formatted in three partitions (e.g., 1234-0001-001). The significance of these partitions is listed below:

a. First partition (*1234*-0001-001): The first partition represents the customer requirement. If this is a new customer requirement, the Request will receive a ticket number with a unique first partition; the second and third partitions will be 1.

b. Second partition (1234-*0001*-001): The second partition represents the instantiation of the CDS device. For example, if three CDS devices were needed for load balancing, the ticket numbers would be 1234-0001-001, 1234-0002-001, and 1234-0003-001. The configuration and customer requirement is the same, but there are three devices meeting this requirement. These devices could be the same configuration at the same location or they could be the same configuration at three different locations.

c. Third partition (1234-0001-*001*): The third partition of the ticket number represents the iteration of the ticket. This number is usually created when a CDS Request is approved to change the configuration or upgrade a previous device. For CDES, this happens often due to the addition of new channels supporting new customers. For example, if pre-existing ticket 1234-0001-001 were upgrading to the next version of RM, the newly assigned ticket number would be 1234-0001-002.

3. Q. What is the different between a CDSA and an ATC?

A. Once a DIACAP package is submitted, reviewed and accepted by the CAO an ATC for the CCSD is issued. The ATC contains the statement "This ATC does not authorize any Cross Domain Solutions, a Separate Cross Domain Solution Authorization Letter will be issued authorizing Cross Domains." A CDSA is issued after DSAWG approval of a CDS contingent upon a current ATC for the CCSD and the ATO, SCQ, and Topology properly referencing the CDS ticket number.

NOTE: *The CDSA expiration date will not exceed the ATC expiration date if the ATC expires prior to the DSAWG approval expiration. Once a new ATC is issued, another CDSA will be issued for the remainder of the DSAWG approval window.*

4. Q. What is the difference between a point-to-point solution and a DISA Cross Domain Enterprise Solution? Am I required to use Enterprise Services?

A. For a point-to-point solution, a customer has a requirement to pass data across security domains, places a request, and purchases their own Cross Domain device to facilitate the information transfer.

Cross Domain Enterprise Services have systems that may be able to facilitate the customer's information transfer requirement. One CDES CDS device could facilitate the transfer of multiple channels from multiple customers. Customers are not required, but are strongly encouraged, to utilize DISA's CDES if their requirement can be met by a CDES Solution. To find out if your requirement could be met by DISA CDES, contact the DISA CDSO at cio-cdso2@disa.mil.

K.5 Points of Contact

All email correspondence with the CDTAB Secretariat should to be sent to cdtab@disa.smil.mil.

Cross Domain Solutions		BRAC Update Effective 16 May 2011
CDS Process Questions	cdtab@disa.smil.mil	cdtab@disa.smil.mil
Updated Enclave Paperwork[9]	cdtab@disa.smil.mil	cdtab@disa.smil.mil
Phone (Commercial)	703-882-2210	703-882-2210, 301-225-2903
Phone (DSN)	312-381-2210	312-381-2210, 312-761-2903
Fax (Commercial)	703-882-2813	703-882-2813
Fax (DSN)	312-381-2813	312-381-2813
Website	www.disa.mil/connect	www.disa.mil/connect

K.6 Additional Policy and Guidance Documents

CJCSI 6211.02C	*Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 (ref a)
DISA Charter	Cross Domain Technical Advisory Board, 18 April 2010
RDAC 2.2, NSA	Risk Decision Authority Criteria
DISA CPG v3.1	Cross Domain Solutions Appendix, April 2011
DoDD 5100.3	*Support of the Headquarters of Combatant and Subordinate Joint Commands*, 15 November 1999 (ref t)

[9] DIACAP paperwork with an ATO expiration date different from that reviewed upon issuance of your last ATC cannot be submitted to cdtab@disa.smil.mil. Please submit the complete DIACAP package to CCAO@disa.smil.mil.

This page intentionally left blank.

APPENDIX L
SME-PED – CLASSIFIED AND UNCLASSIFIED

L.1 SME-PED Description

The Secure Mobile Environment-Portable Electronic Device (SME-PED) is a DISN offering that provides the DoD with the capability that allows wireless NIPRNet and SIPRNet access, to include email and web browsing, in one device. It also provides the user secure and non-secure voice capabilities. Organizations that implement SME-PED must ensure user procedures are in place for use, protection, and control of SME-PED devices.

Some of the service highlights are as follows:

- Converged secure/voice data product
- Secure and non-secure PDA functionality
- Unclassified and Secret secure data
- "Push Email" synchronized with desktop
- Secure and non-secure cellular phone functionality
- Unclassified and "up to" Top Secret secure voice
- Worldwide service capability - GSM/CDMA
- Data at rest - PIN and token

L.2 SME-PED Connection Process

Customers/sponsors that require access to the SME-PED service do not currently follow the connection process identified in this guide. Use of SME-PED is dependent on a SIPRNet connection at the local enclave. Implementation of the SME-PED service requires that a SME-PED server be added to the local SIPRNet enclave. The addition of a server to the local enclave requires an update to the site accreditation package. Once the enclave DAA has approved inclusion of SME-PED into the accreditation boundary, an updated accreditation package should be submitted to the DISA CAO.

L.3 Points of Contact

Connection Approval Office (CAO)		BRAC Update Effective 16 May 2011
Unclassified email	CCAO@disa.mil	CCAO@disa.mil
Classified email	CCAO@disa.smil.mil	CCAO@disa.smil.mil
Phone (Commercial)	703-882-1455	703-882-1455, 301-225-2900/2901
Phone (DSN)	312-381-1455	312-381-1455, 312-761-2900/2901

SME-PED Program Office	
Phone (Commercial)	410-854-1408/1460/1932

L.4 Additional Policy and Guidance Documents

For more information on the SME-PED program, refer to the following website: http://www.disa.mil/services/smeped.html.

APPENDIX M

DISA SERVICE MANAGER POINT OF CONTACT LIST

DISN Service	Information Type	Required Security Level	Connection Purpose (keywords)	Contact Information
SIPRNet	Data	Classified	Operational, C2, Cross Domain Solutions, Narcotics, Anti-drug Network	301-225-2484 DSN (761) ssmo@disa.mil
NIPRNet	Data	Unclassified	Operational, Non-C2	301-225-2083 DSN (761)
DVS (DISN Video Services)	Video	Classified/ Unclassified	VTC capability, DVS-G	703-882-4110 DSN (381) vtcops@disa.mil dvs@disa.smil.mil
DRSN (Defense RED Switch Network)	Voice	Classified	Secure voice, SME-PED, VoSIP, DRSN	703-882-0314 (VoSIP) / x0352 (SME-PED) / x0351 (DRSN) DSN (381)
DSN (Defense Switched Network)	Voice	Unclassified	VoIP, Unclassified Voice, DSN	703-882-0330 DSN (381)
DISN-LES (DISN-Leading Edge Services)	Data	Classified/ Unclassified	Test and Evaluation; R&D	301-225-2463 DSN (761)
RTS (Real Time Services) IO and EoIP (Interoperability and Everything over IP)	Data	Classified/ Unclassified	Converged Voice Video, Data over IP	703-882-0667 DSN (381)
EMSS (Enhanced Mobile Satellite Services)	Voice, Data, Paging, Short Burst Data (SBD)	Unclassified, Classified	Operational, C2, Secure Voice	1-877-449-0600 DSN 312-282-1048 customer.service@gdc4s.com
IC (Intelligence Community)	Data, Voice, Video	Unclassified, Classified	Intelligence specific bandwidth services	703-882-2733/0754 DSN (381)

DISN Service	Information Type	Required Security Level	Connection Purpose (keywords)	Contact Information
DMS (Defense Message System)	Data	Unclassified, Classified	Messaging system, Plain Language Messaging, DMS Security Updates, Plain Language Address Distribution System (PLADS), DMS Asset Distribution System (DADS)	703-882-0503 DSN (381)

Non-DISN Service	Description	Contact Information
DREN/DREN-S (Defense Research and Eng. Network)	Non-DISN Network; provide contact info	703-812-8205 http://www.hpcmo.hpc.mil/Htdocs/DREN/dren-sa.html
MDA (Missile Defense Agency)	Ask customer if connection requires connection to the DISN: If NO, then provide contact info If YES, then follow guidance above to determine which DISN SM should receive this request	703-882-6944 703-882-6906

OSD(NII) Approval Office	Description	Contact Information
OASD(NII)	OSD Approval Letter	703-607-5244

Connection Approval Office	Description	Contact Information	BRAC Update Effective 16 May 2011
CAO	OSD Approval Letter/ Certification and Accreditation Approval Packages	703-882-1455 703-882-2086 ccao@disa.mil ucao@disa.mil	703-882-1455 703-882-2086 301-225-2900/2901 ccao@disa.mil ucao@disa.mil

DISN Connection Process Guide	Description	Contact Information
CPG	Website questions – Unclassified	ucao@disa.mil, ccao@disa.mil
CPG	Website questions – Classified	ucao@disa.smil.mil, ccao@disa.smil.mil

APPENDIX N

REFERENCES

Reference Number	Title
(a) CJCSI 6211.02C	*Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008 http://www.dtic.mil/cjcs_directives/
(b) CJCSI 6215.01C	*Policy For Department Of Defense Voice Networks With Real Time Services (RTS)*, 9 November 2007 http://www.dtic.mil/cjcs_directives/
(c) DoDD 8500.01E	*Information Assurance (IA)*, 24 October 2002 http://www.dtic.mil/whs/directives/
(d) DoDD O-8530.1	*Computer Network Defense*, 8 January 2001 http://www.dtic.mil/whs/directives/
(f) DoDI 8500.2	*Information Assurance (IA) Implementation*, 6 February 2003 http://www.dtic.mil/whs/directives/
(g) DoDI 8510.01	*DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007 http://www.dtic.mil/whs/directives/
(h) DoDI O-8530.2	*Support to Computer Network Defense (CND)*, 9 March 2001 http://www.dtic.mil/whs/directives/
(i) CJCSI 6212.01E	*Interoperability and Supportability of Information Technology and National Security Systems*, 15 December 2008 http://www.dtic.mil/cjcs_directives/
(j) DoDI 8551.01	*Ports, Protocols, and Services Management*, 13 August 2004 http://www.dtic.mil/whs/directives/
(k) CNSSI 4009	*National Information Assurance Glossary*, June 2006 http://www.cnss.gov/full-index.html
(l) CNSS 6	*National Policy on Certification and Accreditation of National Security Systems*, October 2005 http://www.cnss.gov/full-index.html
(m) UCR 2008	*Department of Defense Unified Capabilities Requirements 2008*, December 2008 (signed 22 January 2009) http://www.disa.mil/ucco/
(n) DoDD 8000.01	*Management of the Department of Defense Information Enterprise*, 10 February 2009 http://www.dtic.mil/whs/directives/
(o) DoDI 8100.4	*DoD Unified Capabilities*, 9 December 2010 http://www.dtic.mil/whs/directives/

Reference Number	Title
(p) DoD 5220.22-M	*National Industrial Security Program Operating Manual (NISPOM)*, 28 February 2006 http://www.dtic.mil/whs/directives/
(q) NIST SP 800-37 Rev 1	*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 http://csrc.nist.gov/publications/
(r) DoDI 4630.8	*Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004 http://www.dtic.mil/whs/directives/
(s) ICD 503	*Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation*, 15 September 2008 *http://www.dni.gov/electronic_reading_room.htm*
(t) DoDD 5100.3	*Support of the Headquarters of Combatant and Subordinate Joint Commands*, 15 November 1999 http://www.dtic.mil/whs/directives/

APPENDIX O

ACRONYMS

Acronym	Definition
AA	Accrediting Authority
AAD	Access Approval Document
AIS	Automated Information System
APL	Approved Products List
ASN	Autonomous System Number
ATC	Approval to Connect
ATD	Authorization Termination Date
ATO	Authorization to Operate
BD	Business Development
C&A	Certification & Accreditation
CA	Certifying Authority
CAO	Connection Approval Office
CAP	Connection Approval Process
CC/S/A/FA	Combatant Command, Service, Agency, or Field Activity
CCAO	Classified Connection Approval Office (now referred to as CAO)
CCSD	Command Communications Service Designator
CDA	Cross Domain Appendix
CDRB	Cross Domain Resolution Board
CDS	Cross Domain Solution
CDSAP	Cross Domain Solutions Assessment Panel
CDSO	Cross Domain Solutions Organization
CDTAB	Cross Domain Technical Advisory Board
CIO	Chief Information Officer
CND	Computer Network Defense
CNDS	Computer Network Defense Services
CNDSP	Computer Network Defense Service Provider
COCOM	Combatant Command
CODEC	Coder-Decoder
COMSEC	Communications Security
COTS	Commercial Off-The-Shelf
CPE	Classified Provider Edge
CPG	Connection Process Guide

Acronym	Definition
CTM	Consent to Monitor
CTO	Communications Tasking Order
DAA	Designated Accrediting Authority
DADS	DMS Asset Distribution System
DATC	Denial of Approval to Connect
DGSC	DISN Global Support Center
DDOE	DISA Direct Order Entry
DECC	Defense Enterprise Computing Center
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISN-LES	Defense Information System Network - Leading Edge Services
DITPR	DoD Information Technology Portfolio Repository
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DoD	Department of Defense
DREN	Defense Research and Engineering Network
DRSN	Defense Red Switch Network
DSAWG	Defense IA/Security Accreditation Working Group
DSN	Defense Switched Network
DSS	Defense Security Service
DVS	DISN Video Services
DVS-G	DISN Vide Services – Global
DVS-WS	DISN Video Services – Web Site
EMSS	Enhanced Mobile Satellite Services
EoIP	Everything over Internet Protocol
FOUO	For Official Use Only
FRAGO	Fragmentary Order
FSO	Field Security Operations
FTS	Federal Telecommunications Service
GCA	Government Contracting Authority
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
IA	Information Assurance
IATC	Interim Approval to Connect

Acronym	Definition
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IC	Intelligence Community
ICTO	Interim Certificate to Operate
IDS	Intrusion Detection System
IMUX	Inverse Multiplexer
INFOSEC	Information Security
IO	Interoperability
IOS	Internetworking Operating System
IP	Internet Protocol
IS	Information Systems
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISSE	Information System Security Engineering
IT	Information Technology
JITC	Joint Interoperability Test Command
LAN	Local Area Network
MCU	Multipoint Control Unit
MDA	Missile Defense Agency
MHS	Military Health System
MSL	Multiple Security Level
NA	Not Applicable
NC	Non-Compliant
NIAP	National Information Assurance Partnership
NIC	Network Information Center
NIPRNet	Non-classified Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NS/EP	National Security/Emergency Preparedness
OASD(NII)	Office of the Assistant Secretary of Defense for Networks and Information Integration
OSD	Office of the Secretary of Defense
OTAR	Over The Air Rekey
OWA	Outlook Web Access
PDC	Program Designator Code

Acronym	Definition
PKI	Public Key Infrastructure
PLADS	Plain Language Address Distribution System (PLADS)
PO	Program Office
POA&M	Plan of Action & Milestones
POC	Point of Contact
PPSM	Ports, Protocols, and Services Management
RDAC	Risk Decision Authority Criteria
RFS	Request for Service
RTS	Real Time Services
SBD	Short Burst Data
SCQ	SIPRNet Connection Questionnaire
SDP	Service Delivery Point
SGS	SIPRNet GIAP System
SIP	System Identification Profile
SIPRNet	Secret Internet Protocol Router Network
SM	Service Manager
SME	Subject Matter Expert
SME-PED	Secure Mobile Environment-Portable Electronic Device
SMO	Service Management Office
SNAP	System/Network Approval Process
SSAA	System Security Authorization Agreement
SSC	SIPRNet Support Center
SSE	System Security Engineer
SSM	Single System Manager
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
TCO	Telecommunications Certification Office
TR	Telecommunications Request
TS	Top Secret
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
UC	Unified Capabilities
UCAO	Unclassified Connection Approval Office (now referred to as CAO)
UCDMO	Unified Cross Domain Management Office
USCC	USCYBERCOM

Acronym	Definition
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VOC	Video Operations Center
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VPL	Validated Product List
VPL	Virtual Private LAN
VTF	Video Teleconferencing Facility
WAN	Wide Area Network

This page intentionally left blank.

APPENDIX P

GLOSSARY

Term	Definition
Accreditation Decision	A formal statement by a DAA regarding acceptance of the risk associated with operating a DoD IS and expressed as an ATO, IATO, IATT, or DATO. The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD PKI-certified digital signature. (Ref g)
Approval to Connect (ATC)	A formal statement from the CAO granting approval for an IS to connect to the DISN. The ATC cannot be granted for longer than the period of validity of the associated ATO. An ATO may be issued for up to three (3) years. An ATC will not be granted based on an IATO.
Artifacts	System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the information assurance (IA) posture of the DoD IS, make up the C&A information, and provide evidence of compliance with the assigned IA controls. (Ref g)
Authorization to Operate (ATO)	Authorization granted by a DAA for a DoD IS to process, store, or transmit information; an ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to three (3) years. (Ref g)
Authorization Termination Date (ATD)	The date assigned by the DAA that indicates when an ATO, IATO, or IATT expires. (Ref g)
Connection Approval Process (CAP)	Packages that provide the CAO with the information necessary to make the connection approval decision.
Certification	A comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned IA controls based on standardized procedures. (Ref g)
Certification Determination	A CA’s determination of the degree to which a system complies with assigned IA controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate IA security weaknesses as documented in the IT Security Plan of Action and Milestones (POA&M). (Ref g)
Certifying Authority (CA)	The senior official having the authority and responsibility for the certification of ISs governed by a DoD Component IA program.
Consent to Monitor (CTM)	This is the agreement signed by the DAA granting DISA permission to periodically monitor the connection and assess the level of compliance with IA policy and guidelines.
Connection Approval Process	Formal process for adjudication requests to interconnect information systems.
Connection Approval Office (CAO)	Single point of contact within DISA for all DISN connection approval requests.
Command Communications Service Designator (CCSD)	A unique identifier for each single service including use circuits, package system circuits, and interswitch trunk circuits.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.

Term	Definition
Computer Network Defense Service Provider (CNDSP)	Required by policy to establish or provide for Computer Network Defense Services (CNDS). Support and coordinate the planning and execution of CND, develop national requirements for CND, and serve as the Accrediting Authority (AA) for the CNDS Certification Authorities (CNDS/CA).
Cross Domain Appendix (CDA)	In support of the C&A of a CDS, this appendix defines the security requirements, technical solution, testing, and compliance information applicable to the cross-domain connection.
Cross Domain Solution (CDS)	A form of controlled interface that provides the capability to manually and/or automatically access and/or transfer information between different security domains and enforce their security policies. (Ref k)
Connection Process Guide (CPG)	Step-by-step guide to the detailed procedures that customers must follow in order to obtain and retain connections to the DISN.
Defense Information System Network (DISN)	DoD integrated network, centrally managed and configured to provide long-haul information transfer for all DoD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services.
Defense Information System Network-Leading Edge Services (DISN-LES)	Defense Information System Network-Leading Edge Services (DISN-LES) is a Mission Assurance Category III program designed to pass encrypted unclassified and classified traffic over the Classified Provider Edge (CPE) routers of the DISN, and provide capability for subscriber sites requiring "next generation" network, encryption, software, NETOPS, and advanced services not offered by other DISN Subscription Services (DSS). The network provides a non-command-and-control, risk aware infrastructure identical to the core DISN data services (NIPRNet and SIPRNet).
Denial of Approval to Connect (DATC)	A formal statement by the CAO withholding (in the case of a new connection request) or rescinding (in the case of an existing connection) approval for an IS to connect (or remain connected) to the DISN.
Denial of Authorization to Operate (DATO)	A DAA decision that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted. (Ref g)
Designated Accrediting Authority (DAA)	The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (Ref g)
DISA Defense Enterprise Computing Center (DECC)	Services provided within a backdrop of world-class computing facilities located in both the continental United States (CONUS) and outside of the continental United States (OCONUS
Defense Information Assurance Certification and Accreditation Process (DIACAP)	The DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, federal and DoD requirements.
Defense IA/Security Accreditation Working Group (DSAWG)	Provides, interprets, and approves DISN security policy, guides architecture development, and recommends accreditation decisions to the DISN Flag panel. Also reviews and approves cross domain information transfers (as delegated from the DISN/GIG Flag Panel) or forwards such recommendation(s) to the Flag Panel.

Term	Definition
DIACAP Scorecard	A summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically; it shows the implementation status of a DoD Information System's assigned IA controls (i.e., compliant (C), non-compliant (NC), or not applicable (NA)) as well as the C&A status. (Ref g)
Demilitarized Zone (DMZ)	Physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
Defense Information Systems Agency (DISA) Direct Order Entry(DDOE)	This is the ordering tool for DISN telecommunications services.
DoD Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. It includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (Ref c)
DoD Customer	DoD Combatant Commands, Military Services and Organizations, Agencies, and Field Activities (CC/S/A/FA), which are collectively referred to as DoD Components.
DoD Unified Capabilities (UC) Approved Products List (APL)	List established in response to DoDI 8100.3 *Department of Defense (DoD) Voice Networks*, 16 January 2004 and the *Unified Capabilities Requirements* (UCR 2008) document. Its purpose is to provide Interoperability (IO) and IA-certified products for DoD Components to acquire and to assist them in gaining approval to connect to DoD networks in accordance with policy.
Field Security Operations (FSO)	Produces and deploys IA products, services, and capabilities to combatant commands, services, and agencies to protect and defend the GIG.
GIG Interconnection Approval Process (GIAP)	Electronic process to submit connection information and register a GIG connection.
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Ref c)
IA Certification and Accreditation	The standard DoD approach for identifying information security requirements, providing security solutions and managing the security of DoD information systems. (Ref c)
Information Systems (IS)	Computer-based information systems are complementary networks of hardware/software that people and organizations use to collect, filter, process, create, and distribute data.
Interim Approval to Connect (IATC)	Temporary approval granted by the CAO for the connection of an IS to the DISN under the conditions or constraints enumerated in the connection approval.
Interim Authorization to Operate (IATO)	Temporary authorization granted by the DAA to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision. (Ref g)
Interim Authorization to Test (IATT)	A temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified period within the timeframe and under the conditions or constraints enumerated in the accreditation decision. (Ref g)

Term	Definition
Interim Certificate to Operate (ICTO)	Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.
Internet Protocol (IP)	Protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.
Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (Ref i)
Mission Partners	Those with whom Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments, allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.
Non-DoD Customer	All organizations and entities that are not components of the Department of Defense; this includes contractors and federally funded research and development centers; other USG federal departments and agencies; state, local, and tribal governments; foreign government organizations/ entities (e.g., allies or coalition partners); non-government organizations; commercial companies and industry; academia (e.g., universities, colleges, or research and development centers); etc. (Ref a)
Plan of Action & Milestones (POA&M)	A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses; required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. (Ref g)
Program or System Manager (PM or SM)	The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs. (Ref g)
Request For Service (RFS)	The document, used to initially request telecommunications service, which is submitted by the requester of the service to his designated TCO.
Service Delivery Point (SDP)	The point at which a user connects to the DISN. The DISN provides IA controls up to the SDP. The customer/user is responsible for IA controls outside of the SDP.
System Identification Profile (SIP)	A compiled list of system characteristics or qualities required to register an IS with the governing DoD Component IA program. (Ref g)
Telecommunications Certification Office (TCO)	The activity designated by a federal department or agency to certify to DISA (as an operating agency of the National Communications System) that a specified telecommunications service or facility is a validated, coordinated, and approved requirement of the department or agency, and that the department or agency is prepared to pay mutually acceptable costs involved in the fulfillment of the requirement.

Term	Definition
Telecommunications Service Order (TSO)	The authorization from Headquarters, DISA, a DISA area, or DISA-DSC to start, change, or discontinue circuits or trunks and to effect administrative changes.
Telecommunications Service Request (TSR)	Telecommunications requirement prepared in accordance with chapter 3, DISAC 310-130-1 and submitted to DISA or DISA activities for fulfillment. A TSR may not be issued except by a specifically authorized TCO.
Unified Capabilities (UC)	The seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available Internet Protocol (IP) infrastructure to provide increased mission effectiveness to the warfighter and business communities. UC integrate standards-based communication and collaboration services including, but not limited to, the following: messaging; voice, video and Web conferencing; Presence; and UC clients. (Ref k)
Unified Cross Domain Management Office (UCDMO)	The UCDMO provides centralized coordination and oversight of all cross-domain initiatives across the Department of Defense and the Intelligence Community.
Virtual Private LAN (VPL)	Means to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks.
Wide Area Network (WAN)	A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).

This page intentionally left blank.

Defense Information Systems Agency
Enterprise Connection Division (NSC)
Post Office Box 4502
Arlington, Virginia 22204-4502
www.disa.mil/connect